



Informática para Caixa Econômica Federal - CEF (Técnico Bancário)

Prof. Diego Carvalho, Prof. Marcos Vinícius Alves Franco, Prof. Diego Carvalho

1 Redes de Computadores - Parte 1 - Noções Iniciais

Documento última vez atualizado em 02/01/2024 às 13:14.





Índice

1.1)	Redes de Computadores - Parte 1 - Noções Iniciais - Teoria	3
1.2)	Redes de Computadores - Parte 1 - Tipos de Conexão-Enlace - Teoria	8
1.3)	Redes de Computadores - Parte 1 - Direções de Transmissão - Teoria	10
1.4)	Redes de Computadores - Parte 1 - Modos de Transmissão - Teoria	13
1.5)	Redes de Computadores - Parte 1 - Classificação de Redes - Teoria	16
1.6)	Redes de Computadores - Parte 1 - Meios de Transmissão - Teoria	44
1.7)	Redes de Computadores - Parte 1 - Equipamentos de Redes - Teoria	53
1.8)	Redes de Computadores - Parte 1 - Padrões de Redes - Teoria	80
1.9)	Redes de Computadores - Parte 1 - Internet - Teoria	110
1.10)	Redes de Computadores - Parte 1 - Gerações da Web - Teoria	119
1.11)	Redes de Computadores - Parte 1 - Deep Web e Dark Web - Teoria	129
1.12)	Redes de Computadores - Parte 1 - Internet das Coisas - Teoria	138
1.13)	Redes de Computadores - Parte 1 - Tecnologias de Acesso - Teoria	145
1.14)	Redes de Computadores - Parte 1 - Resumo	169
1.15)	Mapa Mental - Redes de Computadores - Parte 1	194
1.16)	Questões Comentadas - Redes de Computadores - Parte 1 - MULTIBANCAS	200

1.1 Redes de Computadores - Parte 1 - Noções Iniciais - Teoria



Para assistir ao vídeo correspondente, acesse o LDI.

Redes de Computadores

Conceitos Básicos

INCIDÊNCIA EM PROVA: baixíssima



lindu
@humdaora

quando a internet cai e eu fico olhando
para o roteador esperando ela voltar



✓ Quando a internet cai e eu saio do quarto
depois de três dias



Fala, galera! **Vamos iniciar nossos estudos sobre os Conceitos Básicos de Redes de Computadores** – além de ser um assunto de suma importância, ele subsidia tudo que veremos mais à frente sobre Internet. *Beleza?* Agora vamos contar uma história! No Século XIX, enviar uma carta de Londres até Califórnia por meio dos correios demorava entre dois e três meses – isso se você tivesse grana suficiente para pagar pelo envio de cartas. *Incrível, não?*



Hoje em dia, enviar um correio eletrônico demora uma fração de segundos. Isso melhorou a eficiência das indústrias, dinamizou o comércio global e melhorou a economia mundial fazendo com que chegássemos em alta velocidade a praticamente qualquer ponto do planeta. Galera, vocês podem até pensar que os computadores e as redes de computadores sempre andaram juntos, mas não funcionava assim – as redes vieram bem depois!

Durante a década de 1970, os computadores ficavam isolados no mundo – praticamente não se comunicavam. **Nessa época, eles tinham o tamanho de uma geladeira, às vezes de uma sala e, às vezes, até de um andar inteiro de prédios ou universidades.** Os computadores pessoais ainda não tinham se popularizado, apesar de – em 1977 – um cara chamado Steve Jobs ter lançado um microcomputador com teclado integrado e... pasmem... capaz de gerar gráficos **coloridos**.

Enfim, nessa época, **era comum termos um processamento centralizado**, ou seja, um único computador de grande porte – chamado Mainframe – de alto custo e que rodava em geral poucas e simples aplicações. Na década seguinte, com a popularização dos computadores pessoais, as Redes de Computadores foram ganhando espaço, uma vez que as pessoas descobriram que era muito mais interessante compartilhar dados e recursos.

Do processamento que ocorria integralmente centralizado nos computadores de grande porte, **passamos para um processamento distribuído nos computadores pessoais de uma rede.** Dessa forma, em vez de um único mainframe ser responsável por todo processamento, computadores distintos espalhados em uma rede realizavam parte desse trabalho. Dito isso, chegou a hora de saber o conceito de uma rede:

“Uma rede é um conjunto de terminais, equipamentos, meios de transmissão e comutação que interligados possibilitam a prestação de serviços”.

Bem, eu gosto de uma definição mais simples que afirma que uma rede é um conjunto de dispositivos (normalmente conhecidos como nós) conectados por links de comunicação. Em uma rede, um nó pode ser um computador, uma impressora, um notebook, um *smartphone*, um *tablet*, um *Apple Watch* ou qualquer outro dispositivo de envio ou recepção de dados, desde que ele esteja conectado a outros nós da rede.

As primeiras redes de computadores surgiram dentro de organizações – como uma empresa ou um laboratório de pesquisa – para facilitar a troca de informações entre diferentes pessoas e computadores. **Esse método era mais rápido e confiável do que anterior, que consistia em pessoas carregando pilhas e pilhas de cartões perfurados ou fitas magnéticas de um lado para o outro dentro de uma organização.**

Sim, antigamente os dados de um computador ficavam armazenados em pequenos cartões de papel cheio de furinhos chamado cartões perfurados; ou em um rolo enorme de fita magnética. Se você quisesse trocar informações entre pessoas ou equipamentos, **você tinha que transportar pilhas enormes desses cartões perfurados ou de fitas magnéticas até o local onde se encontrava o destinatário.** Já imaginaram isso?



Um segundo benefício das redes de computadores é a capacidade de compartilhar recursos físicos. Por exemplo: em vez de cada computador possuir sua própria impressora, todos em um departamento poderiam compartilhar apenas uma impressora conectada à rede de computadores. Outro uso comum era compartilhar dispositivos de armazenamento, que na época eram muitos caros e não era viável ter um para cada computador.

Como nós podemos resumir tudo isso? **Bem, uma rede de computadores basicamente tem como objetivo o compartilhamento de recursos, deixando equipamentos, programas e principalmente dados ao alcance de múltiplos usuários**, sem falar na possibilidade de servir como meio de comunicação entre pessoas através da troca de mensagens de texto, áudio ou vídeo entre os dispositivos. *Fechado?*

#VamosPraticar#

(UEG / Assembleia Legislativa de Goiás – 2016) Um conjunto de unidades processadoras interconectadas que permite, inclusive, o compartilhamento de recursos tais como impressoras, discos, entre outros, denomina-se:

- a) Time Sharing
- b) Redes de Computadores
- c) Compartilhamento do Windows
- d) Interligação de Redes de Computadores

Comentários: quando a banca diz “*um conjunto de unidades processadoras*”, ela só está usando um nome técnico para “*um conjunto de computadores*”. Portanto, um conjunto de computadores interconectados que permite o compartilhamento de recursos tais como impressoras, discos, entre outros, só pode ser uma... rede de computadores (Letra B).

(PROF. DIEGO / INÉDITA – 2023) Redes de computadores consistem em um conjunto de dispositivos eletrônicos interconectados para compartilhar recursos e informações.

Comentários: essa é uma das definições fundamentais de redes de computadores. As redes de computadores realmente permitem a conexão de dispositivos para compartilhar recursos, como arquivos, impressoras e acesso à internet, além de permitir a troca de informações entre esses dispositivos (Correto).

(PROF. DIEGO / INÉDITA – 2023) Redes de computadores não desempenham um papel fundamental na comunicação e conectividade global na era da informação.

Comentários: as redes de computadores desempenham um papel crítico na comunicação global, conectividade e na disseminação de informações na era da informação – elas são a espinha dorsal da comunicação digital global (Errado).

(PROF. DIEGO / INÉDITA – 2023) As redes de computadores são sistemas centralizados que não permitem a comunicação distribuída.

Comentários: as redes de computadores permitem comunicação distribuída, conectando dispositivos em todo o mundo e permitindo a troca de informações de forma descentralizada (Errado).

(PROF. DIEGO / INÉDITA – 2023) As redes de computadores representam uma infraestrutura de comunicação que possibilita a troca de dados apenas em nível local.

Comentários: redes de computadores não se limitam a nível local; elas permitem a comunicação e a troca de dados em níveis locais, regionais, nacionais e globais, tornando possível a comunicação em alta escala (Errado).

(PROF. DIEGO / INÉDITA – 2023) As redes de computadores servem como um meio para conectar o mundo digital e não têm impacto na vida cotidiana das pessoas.

Comentários: redes de computadores têm um impacto profundo na vida cotidiana das pessoas, desde permitir a comunicação instantânea via internet até fornecer acesso a serviços online, como compras, bancos e mídias sociais (Errado).

#VamosPraticar#

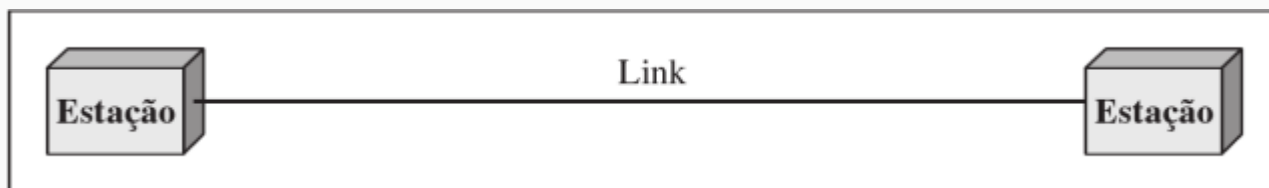
1.2 Redes de Computadores - Parte 1 - Tipos de Conexão-Enlace - Teoria

Tipos de Conexão/Enlace

INCIDÊNCIA EM PROVA: baixíssima

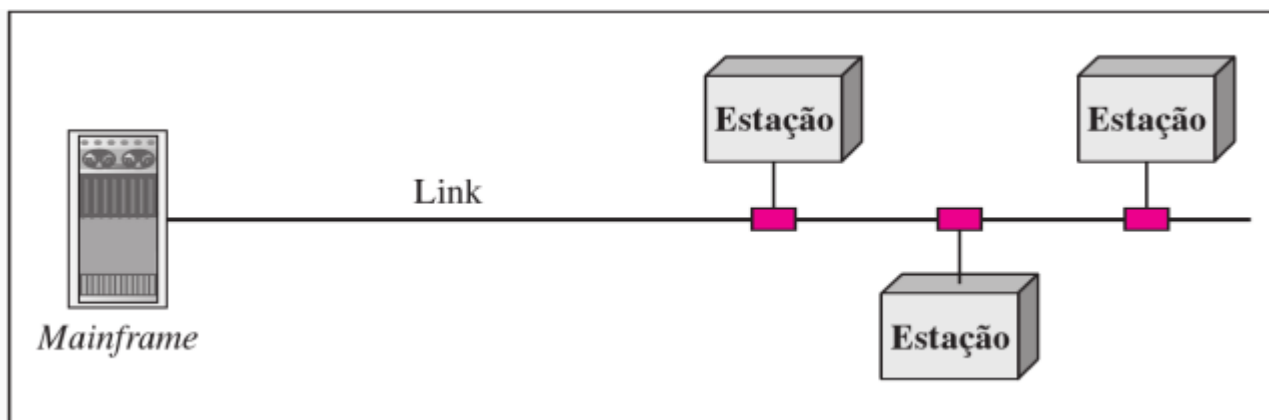
Redes são dois ou mais dispositivos conectados através de links. *O que é um link?* **Também chamado de enlace, trata-se de um caminho de comunicação que transfere dados de um dispositivo para outro.** Para fins de visualização, é mais simples imaginar qualquer link como uma reta entre dois pontos. Para ocorrer a comunicação, dois dispositivos devem ser conectados de alguma maneira ao mesmo link ao mesmo tempo.

Existem dois tipos possíveis de conexão: ponto-a-ponto e ponto-multiponto. Ambos se diferenciam em relação à utilização de um link dedicado ou compartilhado. Como assim, Diego? Um link dedicado é aquele que transporta tráfego de dados apenas entre os dois dispositivos que ele conecta. Exemplo: para que eu acesse a internet, eu compartilho vários cabos subterrâneos espalhados pelo nosso planeta com todas as pessoas que têm acesso à internet.



Nesse contexto, pode-se afirmar que, quando eu acesso à internet, eu utilizo um link dedicado ou um link compartilhado? Galera, eu utilizo um link compartilhado porque o enlace de comunicação é compartilhado com várias pessoas. **No entanto, só é possível ter links dedicados apenas à comunicação entre dois – e apenas dois – dispositivos.** Nesse caso, existe um tipo de conexão conhecido como ponto-a-ponto.

A maioria das conexões ponto-a-ponto utiliza um cabo para conectar dois dispositivos. No entanto, é possível haver links via satélite ou micro-ondas também de forma dedicada. Quando mudamos os canais de televisão por meio da utilização de um controle remoto infravermelho, nós estamos estabelecendo uma conexão ponto-a-ponto entre o controle remoto e o sistema de controle de TV. *Bacana?*



Já em uma **conexão ponto-multiponto**, mais de dois dispositivos compartilham um único **link**. Em um ambiente multiponto, a capacidade do canal de comunicação é compartilhada, seja de forma espacial, seja de forma temporal. Se diversos dispositivos puderem usar o link simultaneamente, ele é chamado de conexão compartilhada no espaço. Se os usuários tiverem de se revezar entre si, trata-se de uma conexão compartilhada no tempo – esse é o modo padrão.

TIPO DE CONEXÃO	DESCRIÇÃO
PONTO-A-PONTO	Conexão que fornece um link dedicado entre dois dispositivos.
PONTO-MULTIPONTO	Conexão que fornece um link compartilhado entre mais de dois dispositivos.

#VamosPraticar#

(PROF. DIEGO / INÉDITA – 2023)

Uma conexão ponto-a-ponto é aquela em que vários dispositivos compartilham o mesmo meio de transmissão, e a comunicação ocorre diretamente entre dois dispositivos, sem a necessidade de compartilhar o meio com outros.

Comentários: a descrição inicial refere-se a uma conexão ponto-multiponto, onde vários dispositivos compartilham o mesmo meio. A conexão ponto-a-ponto é uma conexão direta entre exatamente dois dispositivos – sem compartilhamento (Errado).

(PROF. DIEGO / INÉDITA – 2023)

Uma conexão ponto-multiponto permite a comunicação direta entre dois dispositivos, sem a necessidade de compartilhar o meio de transmissão com outros.

Comentários: uma conexão ponto-multiponto é aquela em que vários dispositivos compartilham o mesmo meio de transmissão, e a comunicação ocorre entre um dispositivo central e vários dispositivos remotos (Errado).

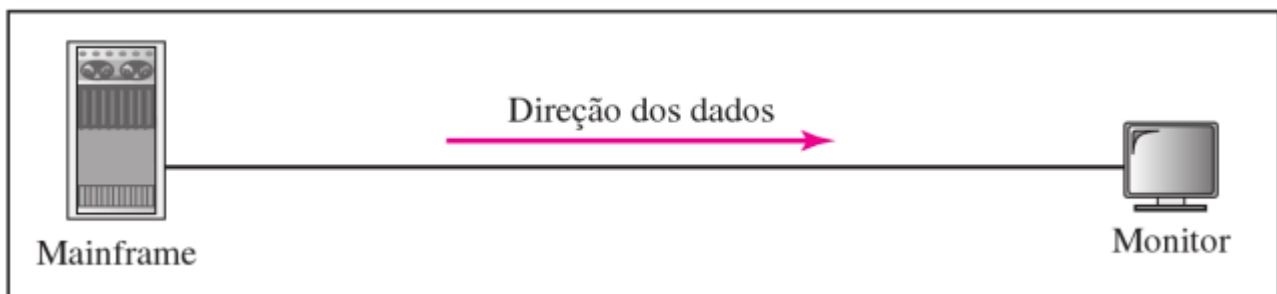
#VamosPraticar

1.3 Redes de Computadores - Parte 1 - Direções de Transmissão - Teoria

Direções de Transmissão

INCIDÊNCIA EM PROVA: baixíssima

Simplex

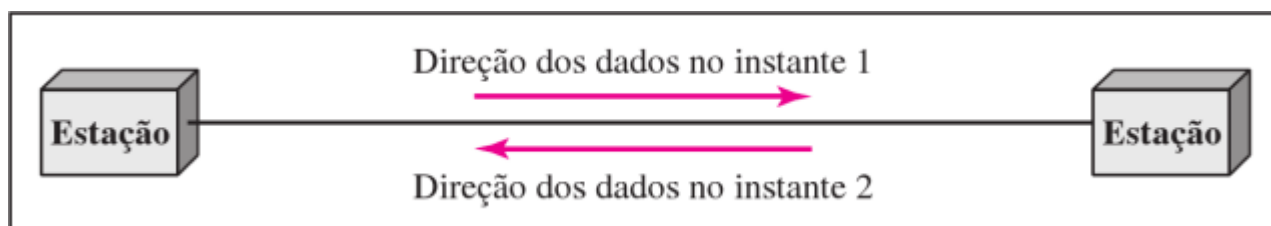


O enlace é utilizado apenas em um dos dois possíveis sentidos de transmissão

Exemplo: TV, Rádio AM/FM, Teclado, etc.

Uma comunicação é dita *simplex* quando há um transmissor de mensagem, um receptor de mensagem e esses papéis nunca se invertem no período de transmissão. Quando você vê TV, sua antena recebe um sinal de um satélite, mas ela jamais envia/transmite sinais para o satélite. Logo, o satélite é o transmissor, sua antena é o receptor, e esses papéis não são trocados – o mesmo serve para Rádio AM/FM ou para o teclado de um computador.

Half-Duplex



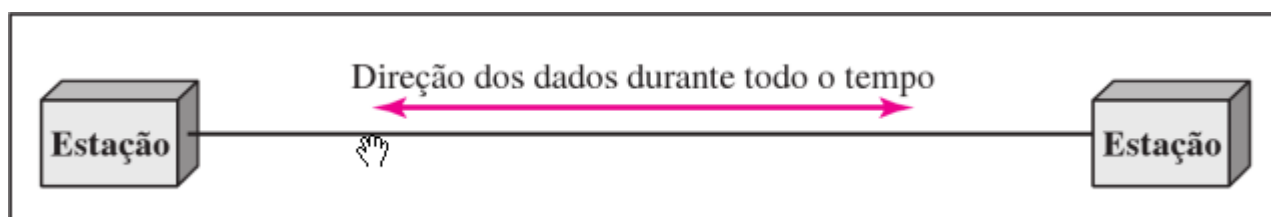
O enlace é utilizado nos dois possíveis sentidos de transmissão, porém apenas um por vez

Exemplo: Walk&Talk e Nextel

Uma comunicação é dita **half-duplex** quando temos um transmissor e um receptor, sendo que ambos podem transmitir e receber dados, porém nunca simultaneamente. Quando você fala em um Walk&Talk com outra pessoa, você pode falar e ela também. Porém, quando você apertar o botãozinho para falar, o receptor apenas ouvirá. Se ele tentar falar junto, a comunicação é cortada e nenhum dos dois se ouve.



Full-Duplex



O enlace é utilizado nos dois sentidos de transmissão simultaneamente

Ex: Celular, VoIP.

Uma comunicação é dita **full-duplex** quando temos um transmissor e um receptor, sendo que ambos podem transmitir e receber dados simultaneamente. Quando você fala com outra pessoa por meio do seu smartphone, ela pode te responder simultaneamente. Você não tem que falar, depois ouvir, depois falar de novo. Vocês dois podem falar juntos sem problema porque se trata de uma transmissão bidirecional.



#VamosPraticar#

(FEPESE / Prefeitura de Balneário Camboriú-SC – 2023)

No contexto de redes de computadores, dentre as formas de transmissão, aquela na qual a comunicação ocorre em uma só direção, com papéis definidos de transmissor (Tx) e receptor (Rx), porém passíveis de inversão, é denominada:

- a) Simples b) Monoplex c) Half Duplex d) Full Duplex e) Auto Duplex.

Comentários: a forma de transmissão na qual a comunicação ocorre em uma única direção, com papéis definidos de transmissor (Tx) e receptor (Rx), mas passíveis de inversão, é denominada Half Duplex (Letra C).

(QUADRIX / CRF-PR – 2022)

Assinale a alternativa que apresenta o tipo de transmissão de dados em que a transmissão é considerada unidirecional, ou seja, um dispositivo é o transmissor e o outro é o receptor.

- a) half-duplex
- b) full-duplex
- c) full-simplex
- d) duplex
- e) Simplex

Comentários: a alternativa que apresenta o tipo de transmissão de dados em que a transmissão é considerada unidirecional, ou seja, um dispositivo é o transmissor e o outro é o receptor é Simplex (Letra E).

#VamosPraticar#

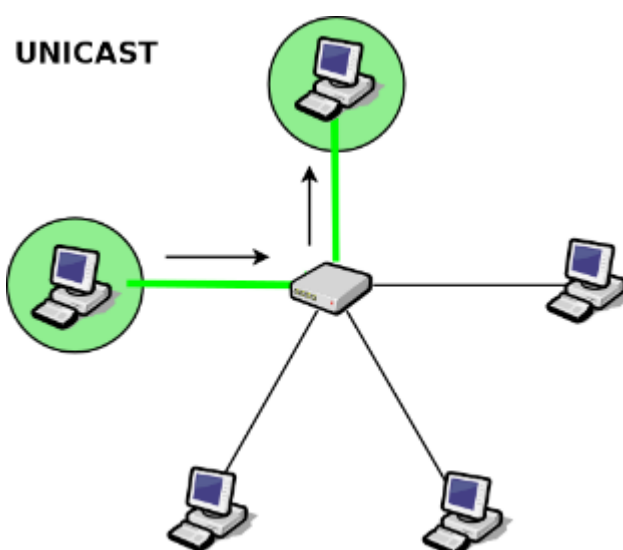
1.4 Redes de Computadores - Parte 1 - Modos de Transmissão - Teoria

Modos de Transmissão

INCIDÊNCIA EM PROVA: baixíssima

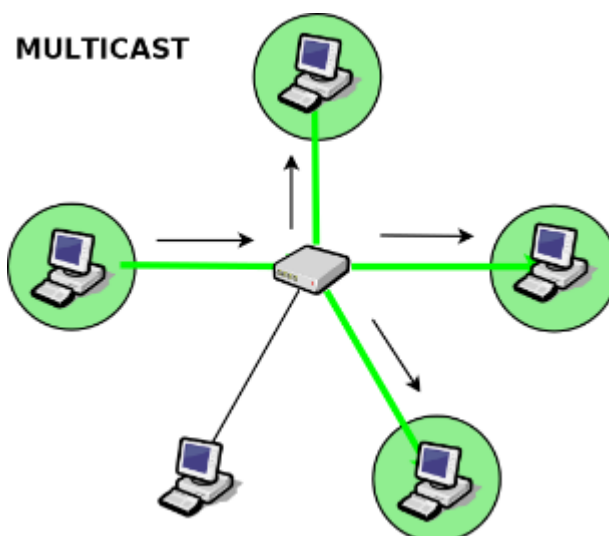
A transmissão de dados em uma rede de computadores pode ser realizada em três sentidos diferentes: *Unicast*, *Multicast* e *Broadcast* ^[1]. Vamos vê-los em detalhes:

Unicast [*uni* = um e *cast* = transmitir]



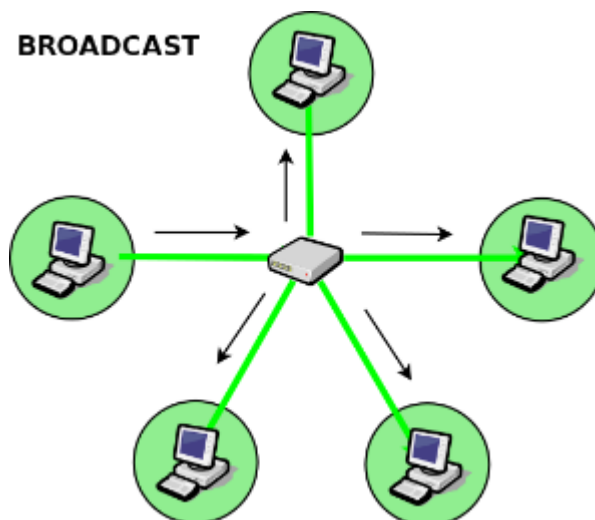
Nessa comunicação, **uma mensagem só pode ser enviada para um destino**. Observem que a primeira estação de trabalho está enviando uma mensagem endereçada especificamente para a 2ª estação de trabalho. Analogamente, quando você envia uma mensagem no Whatsapp para uma pessoa específica, você está enviando uma mensagem *unicast*.

Multicast [*multi* = vários e *cast* = transmitir]



Nessa comunicação, **uma mensagem é enviada para um grupo de destino**. Observem que a primeira estação de trabalho está enviando uma mensagem endereçada para o grupo da 2ª, 3ª e 4ª estações. Analogamente, quando você cria uma lista de transmissão no Whatsapp com um grupo de pessoas e os envia uma mensagem, você está enviando uma mensagem *multicast*.

Broadcast [*broad* = todos e *cast* = transmitir]



Nessa comunicação, **uma mensagem é enviada para todos os destinos**. Observem que a primeira estação de trabalho está enviando uma mensagem endereçada a todas as estações de trabalho. Analogamente, quando você cria uma lista de transmissão no Whatsapp  com todos os seus contatos e os envia uma mensagem, você está enviando uma mensagem *broadcast*.

Cuidado: as questões não prezam por um rigor formal com o nome da classificação. *Como assim, Diego?* Vocês encontrarão questões falando sobre Modo, Tipo, Direção, Sentido, Modalidade ou Fluxo de Transmissão (e ainda há outros nomes). **Cada autor chama de uma maneira assim como cada questão – o que vocês precisam saber é que uma classificação se divide em: Simplex, Half-Duplex e Full-Duplex e a outra é Unicast, Multicast e Broadcast.**

#VamosPraticar#

(QUADRIX / CRBM4 – 2021)

Quanto à difusão, uma rede de computadores pode ser *anycast*, *multicast*, *broadcast* e *unicast*. No modo unicast, a comunicação não pode ocorrer de forma simultânea entre emissor e receptor.

Comentários: quando a comunicação não pode ocorrer de forma simultânea entre emissor e receptor, temos uma comunicação simplex. A comunicação unicast é aquela em que os dados são enviados para um único destinatário (Errado).

(PROF. DIEGO / INÉDITA – 2023)

Unicast é um modo de transmissão onde os dados são enviados para vários destinatários ao mesmo tempo.

Comentários: Unicast é um modo de transmissão em que os dados são para um único destinatário e, não, para vários destinatários ao mesmo tempo – trata-se de uma comunicação ponto a ponto (Errado).

(PROF. DIEGO / INÉDITA – 2023)

Multicast é um modo de transmissão em que os dados são enviados de um único remetente para um grupo específico de destinatários que se inscreveram no grupo multicast.

Comentários: Multicast é, de fato, um modo de transmissão em que os dados são enviados de um único remetente para um grupo específico de destinatários que expressaram interesse ou se inscreveram nesse grupo multicast (Correto).

(PROF. DIEGO / INÉDITA – 2023)

Anycast é um modo de transmissão em que os dados são enviados de um único remetente para o destinatário mais próximo em um grupo de destinatários com o mesmo endereço IP.

Comentários: Anycast é uma técnica de roteamento em que os dados são enviados para o destinatário mais próximo em um grupo de destinatários que compartilham o mesmo endereço IP. Não é necessário entender nada disso agora – é simplesmente entender que esse modo de transmissão existe, é utilizado em casos muito específicos e cai muito raramente em prova (Correto).

(PROF. DIEGO / INÉDITA – 2023)

Unicast é amplamente utilizado em redes de difusão de streaming de vídeo para alcançar muitos assinantes ao mesmo tempo.

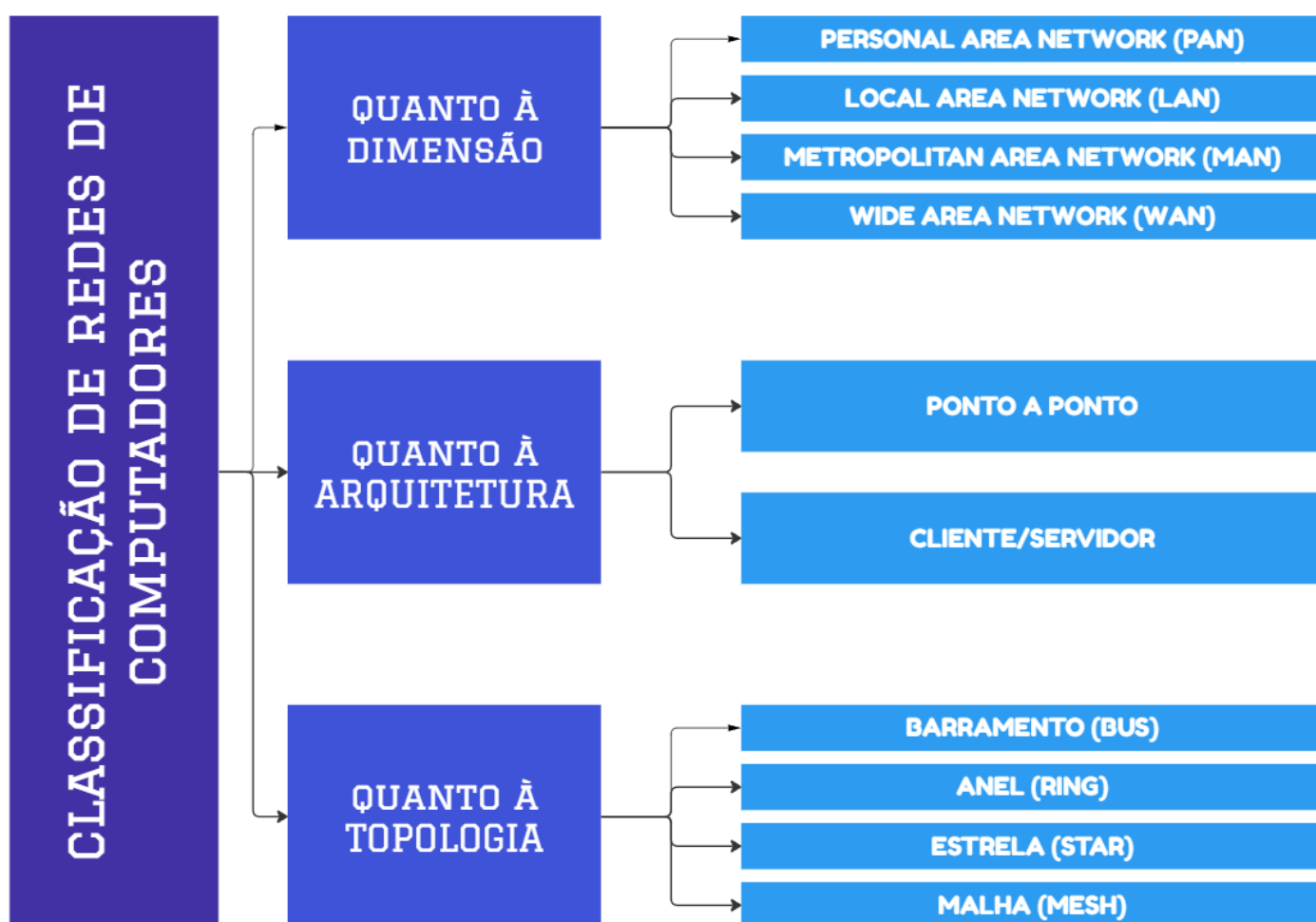
Comentários: Unicast é geralmente inadequado para redes de difusão de streaming de vídeo – Multicast é mais adequado para essa finalidade, uma vez que permite que os dados sejam enviados eficientemente para um grupo de assinantes interessados, economizando largura de banda e recursos da rede (Errado).

#VamosPraticar#

1.5 Redes de Computadores - Parte 1 - Classificação de Redes - Teoria

Classificação de Redes

Neste tópico, vamos falar sobre diversas formas de classificar redes de computadores! Vamos falar da classificação quanto à dimensão, cobertura, tamanho ou área geográfica (PAN, LAN, MAN e WAN); quanto à arquitetura de rede ou forma de interação (ponto-a-ponto e cliente/servidor); e quanto à topologia (barramento, anel, estrela e malha). Existem outras classificações, mas elas não são relevantes para provas de concursos.



Quanto à Dimensão, Tamanho ou Área Geográfica

Uma rede de computadores pode ser classificada quanto à dimensão, tamanho ou abrangência de área geográfica. Galera, nós veremos detalhes sobre as características dessa classificação logo abaixo, no entanto é importante ressaltar uma particularidade a respeito da distância que essas redes de computadores podem abranger. Nós vamos passar algumas noções de distância, mas saibam que não existe nenhuma convenção rígida sobre isso. Fechado?

PAN (Personal Area Network)

INCIDÊNCIA EM PROVA: baixa



DISTÂNCIA

ALGUNS CENTÍMETROS A POUCOS METROS

A **Rede de Área Pessoal** é definida como uma rede de computadores utilizada para conectar e transmitir dados entre dispositivos localizados em uma área pessoal. Pode ser chamada também de WPAN (Wireless Area Network), uma vez que seu principal meio de transmissão é o Bluetooth. Em suma, ela é basicamente uma rede de computadores ou dispositivos que abrange um espaço pequeno (em geral, alguns metros).

Sabe aquele domingo que você leva sua caixinha de som para ouvir uma música na beira da piscina e a conecta ao seu smartphone? **Pois é, isso é uma PAN!** Sabe quando você vai dar aquela corridinha segunda-feira (para se recuperar da cachaça de domingo) e leva seu fone de ouvido sem fio conectado ao seu smartphone também para ouvir uma música? **Adivinha... isso também é uma PAN!** Enfim... entenderam, não é? PAN nem sempre é tratada em questões como uma classificação padrão!

CARACTERÍSTICAS	DESCRIÇÃO
Definição	Rede pessoal que cobre uma área pequena, geralmente dentro de um raio de alguns metros.
Cobertura	Alguns centímetros a poucos metros.
Finalidade	Conectar dispositivos pessoais de curto alcance.
Velocidade	Geralmente de alta velocidade devido à proximidade dos dispositivos.
Tecnologias	Em geral, Bluetooth, Wi-Fi, USB.
segurança	Geralmente mais segura devido à proximidade física.

COMPLEXIDADE	Menos complexa devido à simplicidade da conexão.
ISOLAMENTO	Fácil de isolar problemas devido à proximidade.
APLICAÇÕES	Conexão de dispositivos pessoais, como fones de ouvido sem fio, teclados e mouses.

LAN (Local Area Network)

INCIDÊNCIA EM PROVA: Altíssima



DISTÂNCIA

DE ALGUMAS CENTENAS DE METROS A ALGUNS QUILOMETROS

A **Rede de Área Local** é definida como uma rede de computadores utilizada para conectar e transmitir dados entre dispositivos localizados em uma área de abrangência local. *Quem aí já foi a uma Lan House?* O nome já dá a dica, trata-se de uma LAN. A rede da sua casa também, assim como a rede do andar de um prédio ou a rede de um órgão localizado em um único espaço físico também são redes locais.

Dessa forma, podemos dizer que uma LAN é uma rede de computadores que abrange uma área geográfica relativamente pequena, como um escritório, uma residência, um prédio ou um campus. **Ela é projetada para a interconexão de dispositivos próximos, geralmente dentro de um único local geográfico.** Ela permite a troca de informações, a comunicação eficaz entre os dispositivos conectados e o compartilhamento de recursos (como impressoras e arquivos).

As redes de área local oferecem uma velocidade de comunicação relativamente alta, permitindo uma rápida transferência de dados entre dispositivos, podendo ser configuradas em várias topologias, como barramento, anel ou estrela (mais comum). Além disso, elas podem ser cabeadas ou não. **Em geral, esse tipo de rede possui baixa ocorrência de erros por serem redes pequenas e contidas em um local específico.**

CARACTERÍSTICAS	DESCRIÇÃO
Definição	Rede local que abrange uma área geográfica limitada, como um edifício ou um campus.

Cobertura	De algumas centenas de metros a alguns quilômetros.
Finalidade	Facilitar a comunicação dentro de uma organização local.
Velocidade	Alta velocidade dentro da rede local.
Tecnologias	Em geral, Ethernet e Wi-Fi.
segurança	Pode ser configurada com medidas de segurança, como firewalls.
ComPLEXIDADE	De complexidade moderada, dependendo do tamanho da rede.
ISOLAMENTO	Problemas podem ser isolados com relativa facilidade.
APLICAÇÕES	Uso em escritórios, escolas e redes corporativas locais.

#VamosPraticar#

(AMEOSC / Prefeitura de São João do Oeste-SC – 2023) "No contexto da informática, uma rede consiste em diversos processadores que estão interligados e compartilham recursos entre si". (Tanenbaun, 2014).

Os principais tipos de redes de computadores são: LAN, MAN, WAN, WLAN. Assinale a seguir a alternativa que fala corretamente sobre as redes tipo LAN:

- a) As LANs são redes de computadores que abrangem uma área restrita, como um escritório, uma escola ou um prédio, permitindo a comunicação entre dispositivos próximos.
- b) As LANs são redes de computadores que utilizam apenas tecnologias sem fio (Wi-Fi) para conectar dispositivos dentro de uma área restrita, como um escritório ou uma casa.
- c) As LANs são redes de computadores que conectam dispositivos em longas distâncias, utilizando cabos submarinos e satélites para comunicação global.

d) As LANs são redes de computadores que abrangem uma ampla área geográfica, como um país inteiro, permitindo a conexão entre diferentes regiões.

Comentários: (a) Correto, ela realmente é projetada para abranger uma área geograficamente restrita, como um escritório, uma escola, um prédio ou uma residência, permitindo a comunicação entre dispositivos próximos; (b) Errado, elas podem empregar tanto tecnologias com fio quanto sem fio, dependendo das necessidades e da infraestrutura do ambiente; (c) Errado, redes de longas distâncias são chamadas de WAN (Wide Area Network); (d) Errado, Elas abrangem áreas restritas e não têm a capacidade de conectar diferentes regiões ou países (Letra A).

#VamosPraticar#

MAN (Metropolitan Area Network)

INCIDÊNCIA EM PROVA: Altíssima



DISTÂNCIA

ALGUMAS DEZENAS DE QUILOMETROS

A **Rede de Área Metropolitana** é definida como uma rede de computadores utilizada para conectar e transmitir dados entre dispositivos localizados em locais distintos. Elas possuem abrangência maior que a de uma rede local e menor que a de uma rede extensa – que veremos a seguir. Normalmente uma rede metropolitana resulta da interligação de várias redes locais em uma cidade, formando assim uma rede de maior porte.



Na imagem anterior, temos uma foto aérea de Brasília! Eu não sei se vocês sabem, mas foi aqui que foi criada a Rede de Fast-food Giraffas! Na imagem, temos a localização de dezenas de filiais dessa empresa em uma mesma cidade – **essas filiais podem se conectar formando uma única rede de área metropolitana espalhada em diferentes locais dentro de uma mesma cidade ou metrópole** a uma distância maior que a de uma rede local e menor que a de uma rede extensa.

Características	DESCRIÇÃO
Definição	Rede metropolitana que abrange uma cidade ou uma área metropolitana.
Cobertura	Algumas dezenas de quilômetros
Finalidade	Conectar redes locais dentro de uma área metropolitana.
Velocidade	Velocidade variável, dependendo da infraestrutura da rede.
Tecnologias	Em geral, Ethernet e fibra óptica.
segurança	Maior risco devido à extensão geográfica, exigindo segurança adicional.
ComPLEXIDADE	Moderadamente complexa devido à necessidade de infraestrutura metropolitana.

ISOLAMENTO	Pode ser desafiador isolar problemas devido à extensão geográfica.
APLICAÇÕES	Integração de redes locais em uma área metropolitana.

#VamosPraticar#

(QUADRIX / CRP-MS – 2021) Uma MAN é uma rede doméstica que ocupa o espaço de uma sala. Ela é destinada à conexão de, no máximo, dois computadores.

Comentários: ela não se refere a uma rede doméstica ou uma rede que ocupa o espaço de uma sala. Trata-se de uma rede de comunicação de dados que abrange uma área geográfica maior do que uma rede local, como uma cidade ou uma região metropolitana. Ela é projetada para conectar várias redes locais em uma área geográfica maior, permitindo a comunicação de dados entre essas redes. Não há restrição para o número de computadores em uma rede metropolitana, e seu propósito é fornecer conectividade de rede em uma área metropolitana para instituições, empresas ou organizações (Errado).

#VamosPraticar#

WAN (Wide Area Network)

INCIDÊNCIA EM PROVA: Altíssima



Distância

algumas dezenas de quilômetros

A **Rede de Área Extensa** é definida como uma rede de computadores utilizada para conectar e transmitir dados entre dispositivos localizados em uma grande área geográfica. E quando eu

digo grande, é grande mesmo – podendo ser entre cidades, entre países ou – até mesmo – entre continentes diferentes. O Programa Antártico Brasileiro (PROANTAR) – por exemplo – realiza pesquisas nesse continente e envia os dados para o Brasil por meio de uma rede extensa.



Quando uma empresa possui filiais em cidades ou países diferentes, ela pode criar uma Rede WAN. *Aliás, vocês sabem qual é o melhor e mais clássico exemplo de WAN? A Internet! Sim, a Internet é uma WAN – conforme mostra a imagem ao lado. Outro exemplo seria uma rede entre filiais de empresas localizadas em Brasília e Goiânia – como apresentado na imagem acima. Essa rede formaria o que nós chamamos de rede de área extensa.*

CARACTERÍSTICAS	DESCRIÇÃO
Definição	Uma rede de grande área que pode abranger cidades, países ou até mesmo continentes.
Cobertura	Centenas a milhares de quilômetros.
Finalidade	Conectar redes em diferentes locais geograficamente distantes.
Velocidade	Geralmente menor velocidade devido a longas distâncias.
Tecnologias	Frame Relay, MPLS, Internet.
segurança	Requer medidas de segurança rigorosas devido ao alcance e à exposição a ameaças.
ComPLEXIDADE	Geralmente complexa devido à escala global e aos diferentes tipos de tecnologia.
ISOLAMENTO	Requer ferramentas avançadas para isolar problemas em redes extensas.
APLICAÇÕES	Comunicação em escala regional, nacional ou global.

#VamosPraticar#

(QUADRIX / CFT – 2021) A Internet, que é uma rede global, é um exemplo de rede WAN (Wide Area Network).

Comentários: a Internet é um exemplo clássico de uma rede WAN (Correto).

#VamosPraticar#

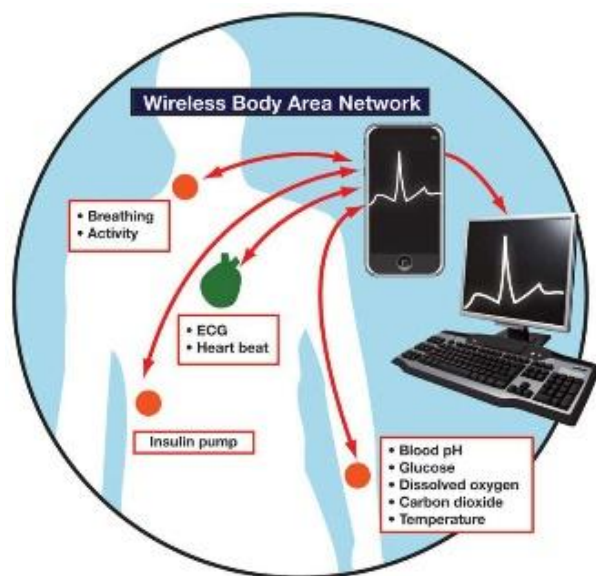
Em suma, a classificação quanto à dimensão pode ser resumida a seguinte tabela:

TIPO	SIGLA	DESCRIÇÃO	DISTÂNCIA
PERSONAL AREA NETWORK	PAN	Rede de computadores pessoal (celular, tablet, notebook, entre outros).	De alguns centímetros a alguns poucos metros.
LOCAL AREA NETWORK	LAN	Rede de computadores de lares, escritórios, prédios, entre outros.	De algumas centenas de metros a alguns quilômetros.
METROPOLITAN AREA NETWORK	MAN	Rede de computadores entre uma matriz e filiais em uma cidade.	Cerca de algumas dezenas de quilômetros.
WIDE AREA NETWORK	WAN	Rede de computadores entre cidades, países ou até continentes.	De algumas dezenas a milhares de quilômetros.

Essas classificações apresentadas possuem uma correspondência quando se trata de um contexto de transmissão sem fio (*wireless*). Em outras palavras, há também WPAN, WLAN, WMAN e WWAN. Por outro lado, as questões de prova nem sempre são rigorosas na utilização desses termos (Ex: é comum enunciados tratando de redes locais sem fio como LAN e, não,

WLAN). Infelizmente, desencanem na hora de resolver questões de prova...

Apenas a título de curiosidade, existem diversas outras classificações menos tradicionais. Duas são bastante interessantes: Body Area Network (BAN) e Interplanetary Area Network (IAN).

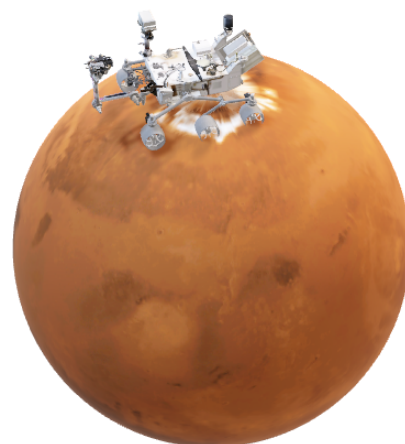


A BAN se trata de uma rede de área corporal que está geralmente relacionada à área de saúde e tem ganhado enorme destaque recentemente.

Dispositivos podem ser implantados dentro do corpo humano ou vestidos em sua superfície. Vocês sabem esses smartwatches que estão na moda agora? Eles são capazes de realizar diversas medidas no seu corpo e enviar para o seu smartphone formando uma rede corporal, no entanto existem dezenas de outras possibilidades...

Existe também uma classificação chamada **Interplanetary Area Network**. Sabe a Curiosity? Ela é um veículo-sonda que está

percorrendo a superfície de Marte desde 2012 e enviando dados para a Terra. Pois é, pode-se classificar a rede formada entre a sonda e nosso planeta como uma IAN – uma Rede de Área Interplanetária cuja distância é de... alguns milhões de quilômetros. Diz se informática não é a melhor disciplina do universo :)



Quanto à Arquitetura de Rede ou Forma de Interação

Antes de entrar nessa classificação, é importante entender alguns conceitos. Primeiro, uma rede é composta por dispositivos intermediários e dispositivos finais. Os dispositivos intermediários são aqueles que fornecem conectividade e direcionam o fluxo de dados em uma rede (Ex: roteadores, switches, etc). Já os dispositivos finais são aqueles que fazem a interface entre o usuário e a rede de computadores (Ex: computadores, notebooks, smartphones, etc).



Na imagem acima, temos quatro dispositivos finais e quatro dispositivos intermediários. Nesse momento, nós vamos tratar apenas dos dispositivos finais – **também chamados de hosts ou sistemas finais**. Esses dispositivos podem ser classificados basicamente em clientes (aqueles que consomem serviços) ou servidores (aqueles que oferecem serviços). Todos nós somos clientes de diversos serviços todos os dias e, às vezes, nem percebemos. Vamos entender isso melhor...

Antigamente, computadores funcionavam de forma isolada. **Foram criadas as redes de computadores com o intuito de otimizar processos, melhor na comunicação e facilitar o compartilhamento de recursos**. Imagine uma empresa com 100 funcionários que precisam com frequência imprimir documentos. *Faz mais sentido comprar uma impressora para cada funcionário ou comprar uma impressora bem mais potente e compartilhá-la com todos?*

Ora, raramente alguém precisa de uma impressora só para si, portanto o compartilhamento de recursos otimizava bastante os custos e processos de uma organização. No entanto, outros recursos podiam ser compartilhados, como softwares, backups, e-mails e – principalmente – dados. **Uma forma eficiente de compartilhar dados é disponibilizá-los em um servidor, que é geralmente uma máquina especializada e poderosa capaz de oferecer serviços a vários clientes.**

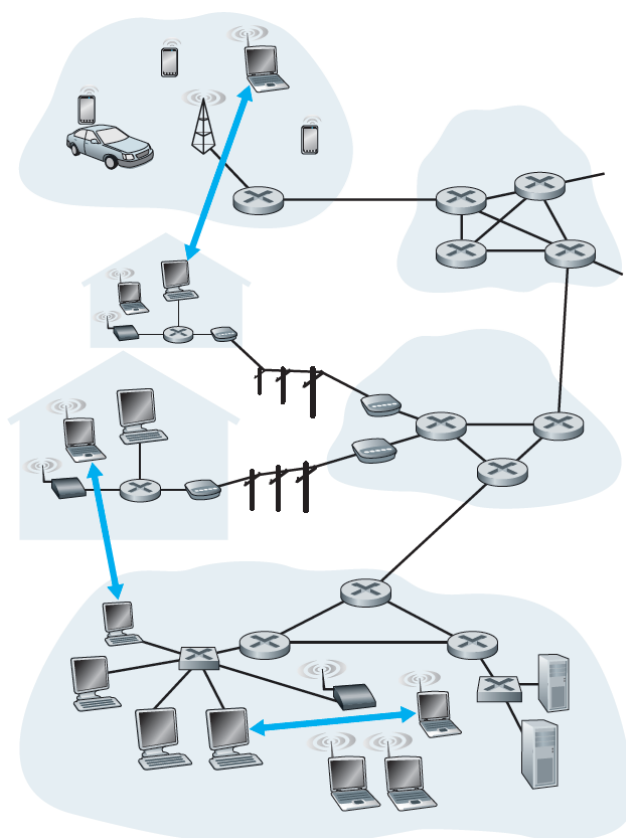
Em contraste, os funcionários da empresa possuem em suas mesas uma máquina mais simples chamada de cliente. *Essas máquinas mais simples acessam dados que estão armazenados aonde?* No servidor! E tanto os clientes quanto os servidores estão conectados entre si por uma rede. Como na vida real, cliente é o aquele que consome algum serviço ou recurso; e servidor é aquele que fornece algum serviço ou recurso. *Simples, não?*

Informalmente, clientes costumam ser computadores de mesa, notebooks, smartphones e assim por diante; ao passo que servidores costumam ser máquinas mais poderosas, que armazenam e distribuem páginas web, vídeo em tempo real, transmissão de e-mails e assim por diante. Hoje, a maioria dos servidores dos quais recebemos resultados de busca, e-mail, páginas e vídeos reside em grandes centros de dados chamados **Datacenters**. Agora nós podemos estudar as arquiteturas!

Rede Ponto-a-Ponto

INCIDÊNCIA EM PROVA: baixa

Também chamada de Rede Par-a-Par ou Peer-to-Peer (P2P), **trata-se do modelo não hierárquico de rede mais simples em que máquinas se comunicam diretamente, sem passar por nenhum servidor dedicado, podendo compartilhar dados e recursos umas com as outras**. Essas redes são comuns em residências e entre filiais de empresas, porque demandam



um baixo custo, são facilmente configuráveis, escaláveis e possibilitam altas taxas de velocidade.

Notem pela imagem que não há uma hierarquia entre os dispositivos finais – todas as máquinas são iguais e, por essa razão, são chamadas de pares (ou peers). Observem também que afirmar que as máquinas se comunicam diretamente não significa que exista um link dedicado entre elas, significa que não há um servidor intermediando a comunicação. **A classificação quanto à arquitetura trata dos papéis que um dispositivo final pode exercer e, não, da conexão entre os dispositivos.**

Nesse tipo de rede, todas as máquinas oferecem e consomem recursos umas das outras, atuando ora como clientes, ora como servidoras. No entanto, nem tudo são flores! Dependendo do contexto, o gerenciamento pode ser bastante

complexo. Quando essa arquitetura é utilizada em redes domésticas com poucos computadores e cuja finalidade é compartilhar impressoras, trocar arquivos e compartilhar internet – não há problema [2].

Por outro lado, quando utilizada em redes de grandes organizações com muitos usuários, o gerenciamento pode ser problemático e sua utilização pode se tornar insegura (por não contar com serviços de autenticação, criptografia, controle de acesso, entre outros). Galera, existem diversas aplicações que utilizam a arquitetura ponto-a-ponto para compartilhar arquivos. Quem já ouviu falar de BitTorrent?

Trata-se de um protocolo de comunicação que utiliza um modelo P2P para compartilhar arquivos eletrônicos na Internet. Diversos softwares utilizam esse protocolo para permitir o download/upload de arquivos, programas, músicas, vídeos e imagens entre usuários. **Em geral, trata-se de um compartilhamento ilegal que favorece a pirataria – inclusive é proibido em diversos países.**

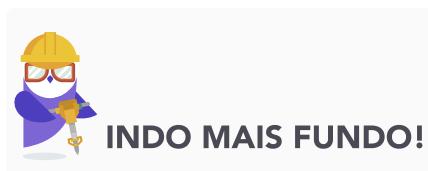
Por anos, a indústria fonográfica e cinematográfica lutou na justiça para impedir a utilização desse tipo de serviço por conta dos prejuízos incalculáveis das gravadoras de discos e produtoras de filmes. *Por que não deu certo, professor?* Pessoal, se esse serviço utilizasse um modelo cliente/servidor, bastava derrubar o servidor que estava disponibilizando os arquivos aos usuários.

No entanto, em uma rede P2P, todas as máquinas são servidores e clientes...

Galera, esse modelo possui uma arquitetura descentralizada em que não existe um repositório central armazenando os arquivos. *E onde estão os arquivos, professor?* **Eles estão espalhados nas máquinas de milhares de usuários ao redor do mundo.** Vamos imaginar um cenário em que eu estou fazendo o download de uma música da máquina de um usuário chamado João. No meio do download, acaba a energia na casa do João. *E agora? Perdi tudo? Já era?*

Nada disso, o software imediatamente busca outro usuário – que também possua a música – e prossegue o download normalmente. Enfim... desistiram de tentar acabar com esse tipo de serviço e atualmente continua bem simples baixar filmes que estão atualmente no cinema. **Claro que é importante tomar cuidado porque os arquivos compartilhados podem conter códigos maliciosos e, assim, infectar um computador ou permitir que ele seja invadido.**

Por fim, é importante mencionar que tratamos acima da Arquitetura P2P Pura. Nesse caso, ela é completamente descentralizada e não há um elemento central, sendo o completo oposto do modelo cliente-servidor. Por conta dos problemas de gerenciamento, foi criada a Arquitetura P2P Híbrida, que possui alguns nós especiais (chamados supernós) para realizar ações de coordenação (Ex: concede acesso, indexar dados compartilhados, liberar busca por recursos, etc).



O termo ponto-a-ponto costuma confundir porque pode ser utilizado em dois contextos com significados diferentes. No contexto de **Tipos de Conexão**, ele pode ser utilizado como contraponto ao enlace ponto-multiponto, ou seja, trata-se de um link dedicado entre dois dispositivos, em contraste com o enlace ponto-multiponto, em que o link é compartilhado entre dispositivos. Já vimos isso...

No contexto de **Arquitetura ou Forma de Interação**, ele pode ser utilizado como contraponto ao modelo cliente/servidor. Nesse caso, trata-se de uma máquina que é simultaneamente cliente e servidor, diferente do modelo cliente/servidor, em que uma máquina ou é um cliente ou é um servidor. Vamos resumir para que vocês nunca mais confundam esses termos:

Se existe um link dedicado entre dois dispositivos, trata-se de um tipo de **conexão ponto-a-ponto**. Por outro lado, se um mesmo dispositivo pode exercer função de cliente ou servidor em diferentes momentos, trata-se de um tipo de **arquitetura ponto-a-ponto**. O nome utilizado é exatamente o mesmo, porém tem significados diferentes dependendo do contexto utilizado.

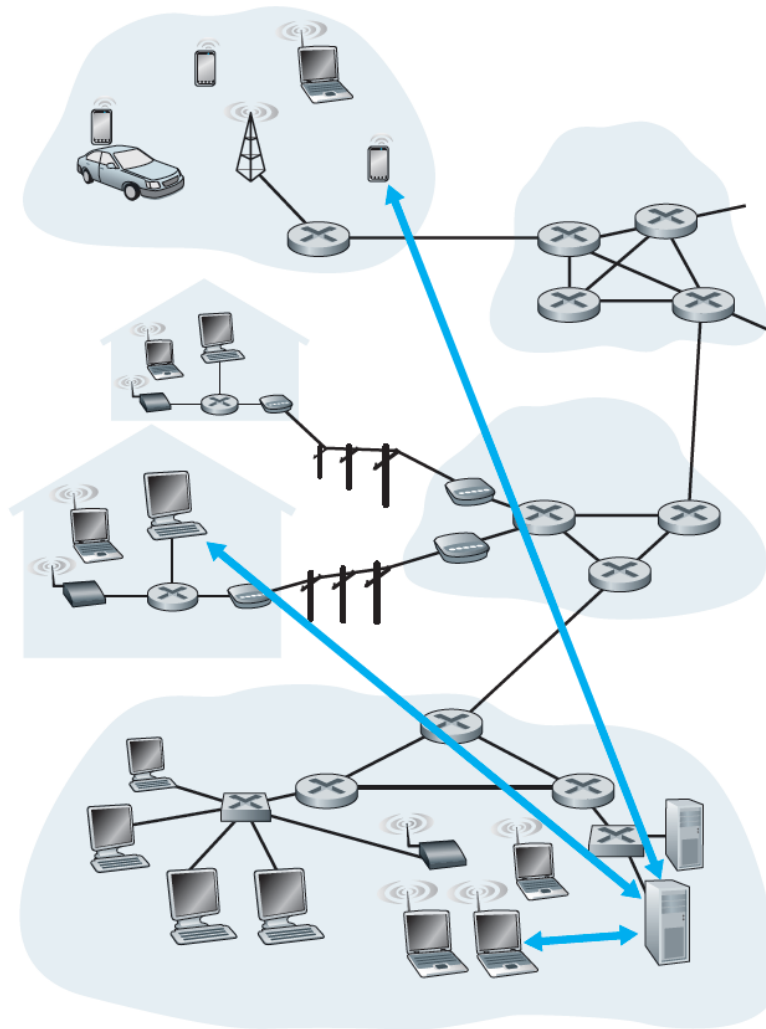
(IDIB / Câmara de Planaltina-GO – 2021 – Letra C) Peer-to-peer (do inglês par-a-par ou simplesmente ponto-aponto, com sigla P2P) é uma arquitetura de redes de computadores onde um dos pontos ou nós da rede funciona como servidor central, compartilhando os serviços e dados entre os demais nós da rede.

Comentários: na arquitetura P2P, não há um servidor central que compartilhe serviços e dados entre os nós da rede. Em vez disso, os nós da rede (ou pares) são igualmente responsáveis por compartilhar recursos e informações entre si, sem depender de um servidor central (Errado).

#VamosPraticar#

Rede Cliente/Servidor

INCIDÊNCIA EM PROVA: média



Trata-se um modelo hierárquico de redes mais complexo, porém potencialmente mais robusto e confiável. **Nesse modelo, existe uma máquina especializada, dedicada e geralmente remota**, respondendo rapidamente aos pedidos vindos dos demais computadores da rede – o que aumenta bastante o desempenho de algumas tarefas. É a escolha natural para redes grandes, como a Internet, que funciona tipicamente a partir do Modelo Cliente/Servidor. Observem na imagem anterior que há diversos dispositivos clientes se comunicando diretamente com um único servidor – um cliente jamais se comunica diretamente com outro cliente.

Ao contrário do que ocorre nas redes par-a-par, os computadores que funcionam como clientes – em regra – não fornecem recursos e serviços aos outros computadores da rede. Que servidores são esses, Diego?

Galera, existem vários tipos de servidores, como por exemplo: servidor de impressão, servidor de e-mails, servidor de arquivos, servidor de comunicação, servidor de banco de dados, servidor de páginas web, entre outros.

Quer um exemplo? Quando você faz o download um vídeo no site do Estratégia Concursos, você está consumindo um recurso do servidor do Estratégia. Sim, o Estratégia possui uma máquina especializada chamada de servidor, onde fica hospedado o seu site. **Quando você faz**

o download da sua aula de informática, você está exercendo um papel de Cliente – e quem fornece o recurso solicitado por você está exercendo o papel de Servidor.

#VamosPraticar#

(CESPE / DP-DF – 2022) Em ambiente cliente-servidor, os clientes se conectam aos servidores para obter acesso aos recursos compartilhados.

Comentários: nessa arquitetura, os servidores fornecem serviços ou recursos e os clientes solicitam e utilizam esses recursos por meio da conexão com o servidor (Correto).

(QUADRIX / COFECI – 2017) Os principais componentes da arquitetura cliente-servidor são um conjunto de servidores, um conjunto de clientes e uma rede.

Comentários: de fato, os principais componentes são clientes, servidores e uma rede (Correto).

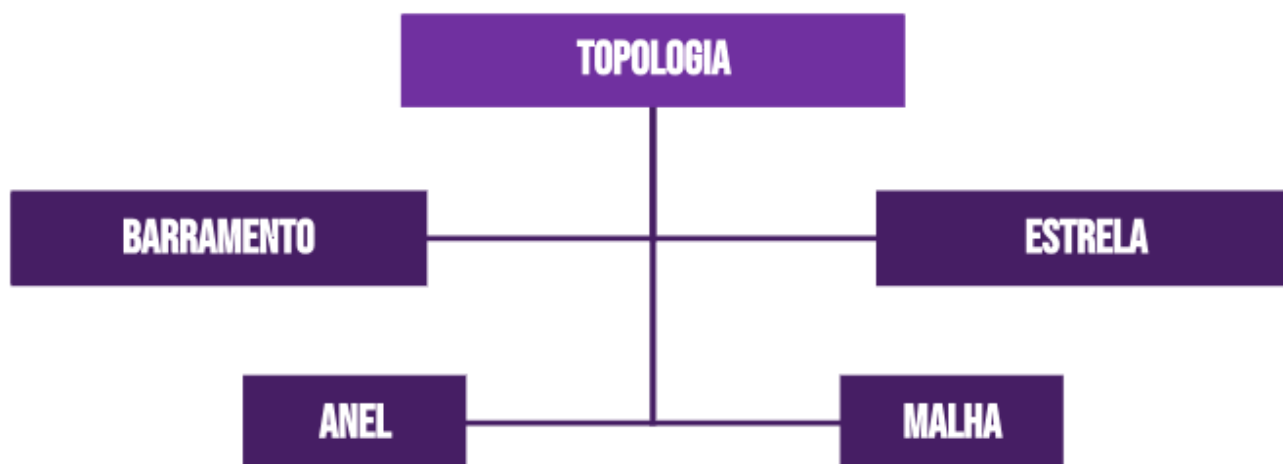
#VamosPraticar#



Para ouvir ao áudio correspondente, acesse o LDI.

Quanto à Topologia (*Layout*)

Quando falamos em topologia, estamos tratando da forma como os dispositivos estão organizados. Dois ou mais dispositivos se conectam a um link; dois ou mais links formam uma topologia. A topologia é a representação geométrica da relação de todos os links e os dispositivos de uma conexão entre si. Existem quatro topologias básicas ^[3]possíveis: barramento, estrela, anel e malha. No entanto, vamos primeiro entender a diferença entre topologia física e lógica.



A topologia lógica exibe o fluxo de dados na rede, isto é, como as informações percorrem os links e transitam entre dispositivos – lembrando que links são os meios de transmissão de dados. Já a topologia física exibe o layout (disposição) dos links e nós de rede. **Em outras palavras, o primeiro trata do percurso dos dados e o segundo trata do percurso dos cabos, uma vez que não necessariamente os dados vão percorrer na mesma direção dos cabos.**

TIPO DE TOPOLOGIA	DESCRIÇÃO
FÍSICA	Exibe o layout (disposição) dos links e nós de rede.
LÓGICA	Exibe o fluxo ou percurso dos dados na rede.



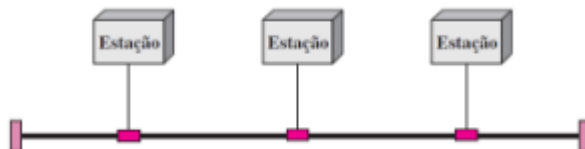
Se uma questão de prova não deixar explícito em sua redação qual é o tipo de topologia, pode-se assumir que ela se refere à **Topologia Física e – não – à Topologia Lógica!**

Barramento (Bus)

INCIDÊNCIA EM PROVA: ALTA

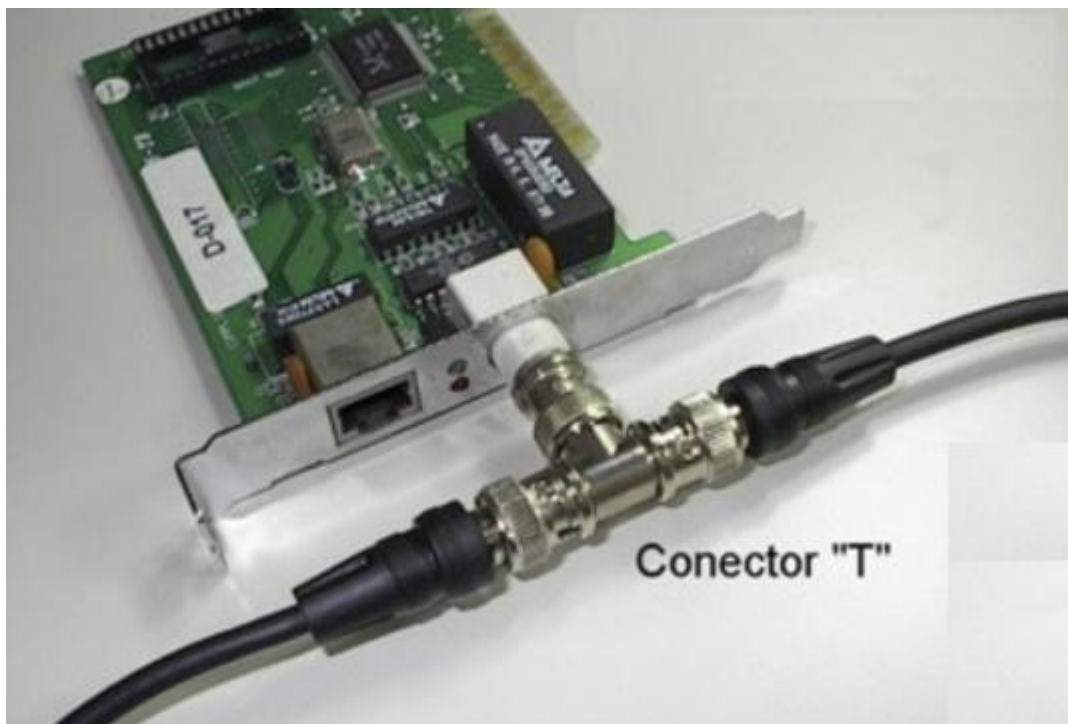
Nessa topologia, todas as estações ficam conectadas ao mesmo meio de transmissão em uma conexão ponto-multiponto. [4] Qual seria esse meio de transmissão, professor?

Trata-se de um cabo coaxial, que veremos em detalhes mais adiante. Notem na imagem seguinte que temos um único enlace compartilhado em que diversos nós se ligam por meio de conectores – o nome desse enlace é *backbone* ou espinha dorsal.



Qual é a consequência de ter um único enlace compartilhado por todos os nós da rede? **Galera, um sinal gerado por um nó de origem qualquer se propagará por todo o barramento em ambas as direções e, portanto, será recebido por todos os demais nós em um modo de transmissão conhecido como *broadcast* – que nós já estudamos.** Então, todos os nós acessarão dados mesmo que não sejam os destinatários originais da mensagem? Calma, não é bem assim...

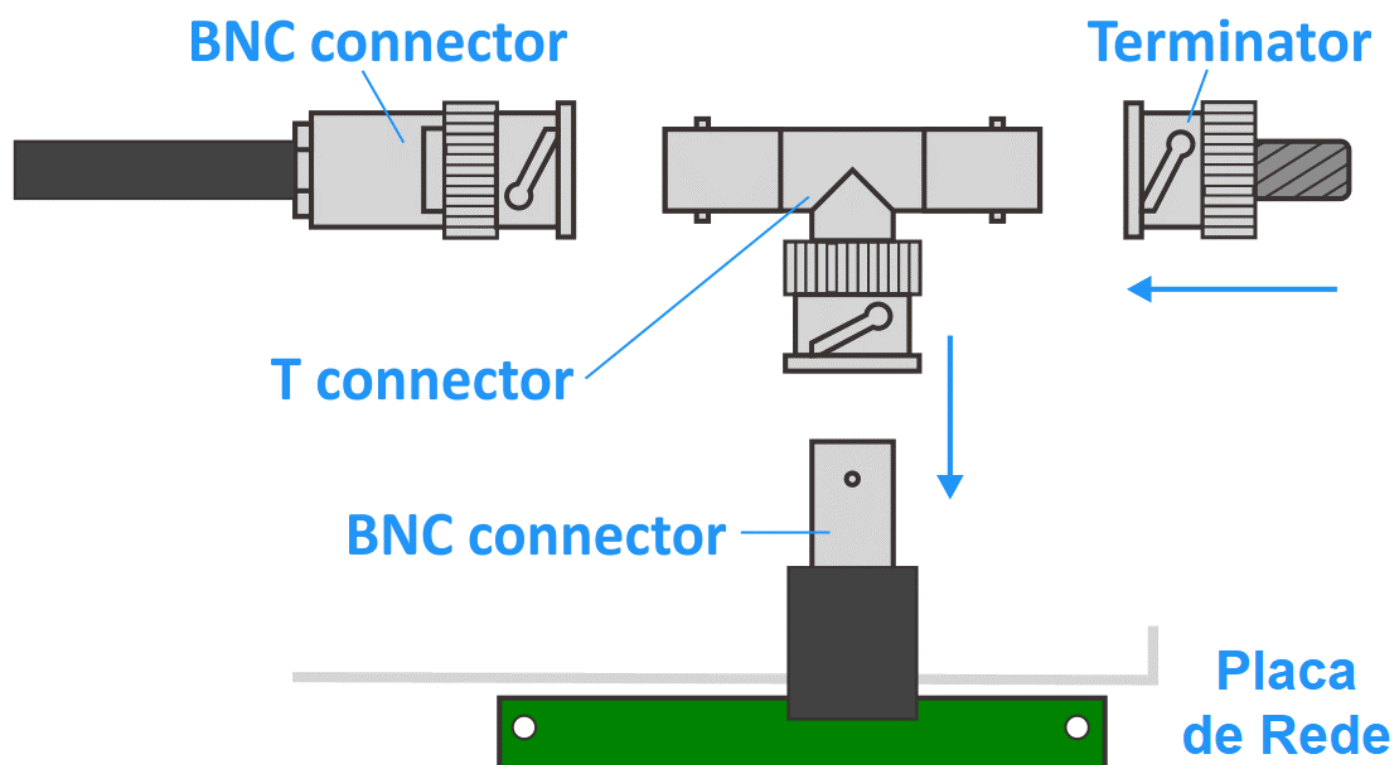
Cada estação de trabalho é conectada ao backbone por meio de uma placa de rede, que tem a responsabilidade de fazer a interface entre a estação de trabalho e o enlace (cabo coaxial). Essa placa de rede receberá os dados, mas somente acessará aqueles que foram endereçados a ela. Em suma: dados são enviados em *broadcast* e recebidos por todas as máquinas conectadas ao *backbone*, porém somente as estações a quem os dados foram endereçados poderão acessá-los.



Outra característica dessa topologia é que todas as estações de trabalho podem enviar dados em qualquer direção, mas jamais simultaneamente. Quando uma estação de trabalho estiver transmitindo dados, todas as outras devem ficar em espera até que ela finalize e que o barramento fique disponível. Só então, outra estação poderá enviar dados. **Em outras palavras, essa topologia trabalha com uma direção de transmissão half-duplex.**

Professor, o que ocorre se duas estações esperarem o barramento ficar disponível e enviarem dados ao mesmo tempo? **Nesse caso, ocorrerá o que chamamos de colisão, isto é, o sinal enviado por uma estação colidirá com o sinal enviado por outra estação.** Vocês se lembram do walk&talk? Como ele também é half-duplex, se duas pessoas falarem simultaneamente, ocorrerá uma colisão e as pessoas não conseguirão se comunicar. *E como resolve isso, professor?* Veremos mais para frente...

Além disso, uma falha ou ruptura no cabo de backbone implica a interrupção da transmissão, até mesmo entre os dispositivos que se encontram do mesmo lado em que ocorreu o problema. *Professor, não entendi muito bem!* **Galera, imaginem que nós temos um varal com diversas roupas penduradas.** Caso haja um rompimento do varal, todas as roupas caem; no entanto, caso haja um problema apenas no pregador de uma roupa e ela cair, nada acontece com o restante.



Vantagens: facilidade de instalação e economia de cabeamento. Em outras palavras, como se trata de apenas de um conjunto de nós conectados a um único cabo, trata-se de uma fácil instalação, além de uma patente economia de cabeamento. **Desvantagens: aumento do atraso e dificuldade de isolar falhas.** Como o link é compartilhado, quanto maior o número de máquinas, maior o atraso (delay) na comunicação e menor o desempenho da rede.

CARACTERÍSTICAS	DESCRIÇÃO
Definição	A topologia em barramento é um design de rede em que todos os dispositivos compartilham um único cabo (<i>backbone</i>).

Escalabilidade	Menos escalável, pois a adição de novos dispositivos pode resultar em colisões de dados.
Confiabilidade	Menos confiável, pois uma falha em qualquer ponto do barramento pode afetar toda a rede.
Desempenho	O desempenho pode degradar quando muitos dispositivos tentam acessar o barramento ao mesmo tempo.
manutenção	A manutenção é relativamente fácil, pois é fácil identificar o ponto de falha no cabo compartilhado.
Complexidade	Menos complexa de implementar, pois envolve um único cabo, mas pode se tornar complicada em redes maiores.
Latência	A latência (atraso na comunicação de uma rede) é variável, dependendo do tráfego da rede. Pode ocorrer colisão de dados que exige retransmissões.
Segurança	Menos segura, uma vez que qualquer dispositivo pode "ouvir" todas as comunicações na rede.
Isolamento de problemas	Problemas podem ser isolados com relativa facilidade, pois é possível localizar fisicamente o ponto de falha no barramento.
Tipos de aplicação	Adequada para redes menores, onde o tráfego é limitado, como redes domésticas ou de laboratórios.

#VamosPraticar#

(QUADRIX / CREFITO-CE – 2022) Assinale a alternativa que apresenta a topologia física de rede de computadores em que há a utilização de um único cabo backbone, que é terminado em ambas as extremidades, e cujos hosts são conectados diretamente a esse cabo.

- a) topologia em anel
- b) topologia em estrela
- c) topologia hierárquica

- d) topologia em malha
- e) topologia em barramento

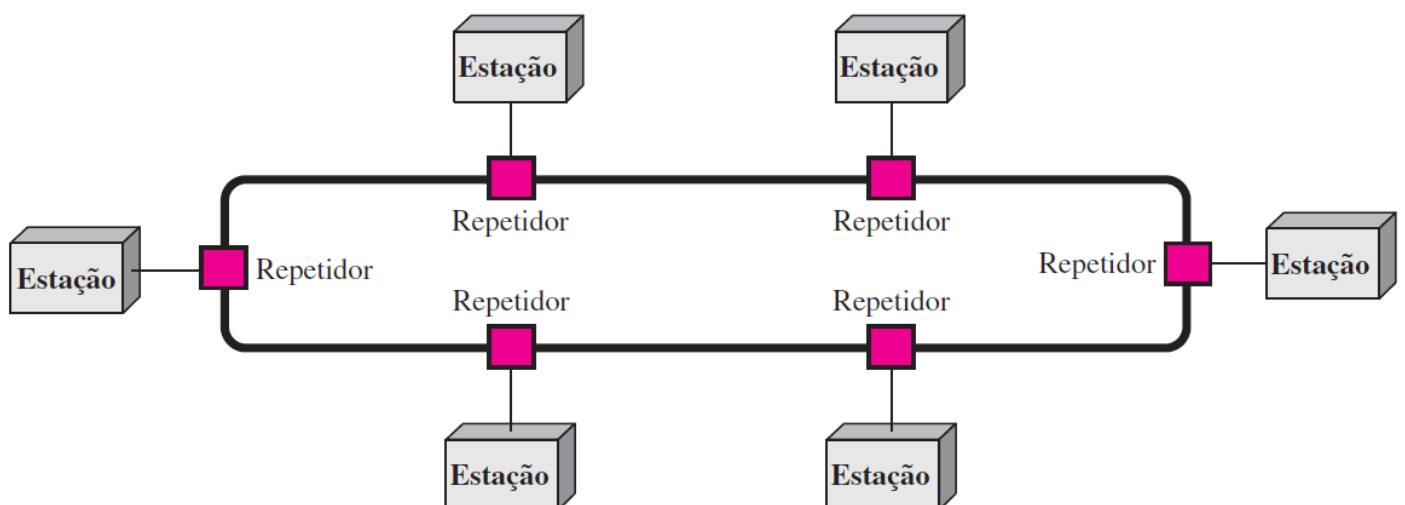
Comentários: a questão trata da topologia em barramento, em que os dispositivos são conectados a um único cabo de backbone, que atua como o canal de comunicação principal. Esse cabo é terminado em ambas as extremidades. Os dispositivos, como computadores ou outros dispositivos de rede, são conectados diretamente a esse cabo. Quando um dispositivo envia dados, esses dados são transmitidos por todo o cabo e todos os dispositivos na rede recebem esses dados. No entanto, apenas o dispositivo de destino apropriado processa os dados, enquanto os outros dispositivos simplesmente os ignoram (Letra E).

#VamosPraticar#

Anel (Ring)

INCIDÊNCIA EM PROVA: média

Nessa topologia, **cada dispositivo tem uma conexão ponto-a-ponto com outros dois dispositivos conectados lado a lado**, e fazendo uso de uma comunicação com transmissão unidirecional (chamada *simplex*). Nesse caso, a mensagem circula o anel, sendo regenerada e retransmitida a cada nó, passando pelo dispositivo de destino que copia a informação enviada, até retornar ao emissor original. Nesse momento, o link é liberado para que possa ser utilizado pelo nó seguinte.



Imagine que um dispositivo deseje enviar mensagem para outro dispositivo do anel. Ele enviará para o dispositivo ao lado; ele verificará que não é o destinatário da mensagem e repetirá a mensagem para seu dispositivo ao lado (**por isso os repetidores**); o próximo dispositivo fará o

mesmo procedimento até chegar ao dispositivo de destino, que receberá os dados e enviará uma mensagem para o dispositivo remetente original para informá-lo de que recebeu os dados.

Dessa forma, pode-se afirmar que os dados são transmitidos em *broadcast*, isto é, dados enviados em uma rede com essa topologia são recebidos por todos os outros dispositivos.

Outra característica interessante é a ausência de colisões. *Como assim, Diego?* Guardem na memória: colisões só ocorrem quando a direção de transmissão é *half-duplex* – jamais ocorre quando a direção de transmissão é *simplex* ou *full-duplex*.

Professor, ainda assim não ocorreria aquele problema de duas máquinas enviarem dados ao mesmo tempo causando colisão? Não, porque a topologia em anel utiliza um envelope de dados chamado Token! Trata-se de um envelope para transmissão de dados que permanece circulando pelo anel até que alguma estação de trabalho que deseje transmitir dados a outra estação de trabalho o capture. *Como é, Diego?*

Pessoal, existe uma modalidade do atletismo chamada Corrida de Revezamento. Quatro atletas percorrem uma pista circular segurando um bastão: o primeiro corre e passa o bastão para o segundo; o segundo corre e passa o bastão para o terceiro; o terceiro corre e passa o bastão para o quarto; e o quarto corre até o final do circuito. Em outras palavras, um atleta somente pode correr caso ele esteja com o bastão em suas mãos. **Aqui funciona de maneira semelhante...**

Uma estação de trabalho somente pode enviar dados quando estiver de posse do token. Em suma, um token fica circulando pelo anel. Quando alguma estação de trabalho deseja enviar dados, ela captura o token, insere seus dados dentro dele e o envia para a estação adjacente, e assim por diante até chegar ao destinatário final. Esse recebe o envelope, verifica que ele é o destinatário do token, captura os dados e insere dentro do envelope um sinal de recebimento.

O envelope continua percorrendo o anel para a próxima estação, e a próxima, e a próxima, até chegar à estação que enviou os dados. **Essa estação abre o envelope, verifica o sinal recebido, confirma que a estação de destino recebeu as informações enviadas e devolve o token para a rede para que ele continue circulando pelo anel.** Quando outra estação quiser enviar outra mensagem, é só capturar o *token* e fazer o mesmo processo. Assim, não há chances de colisões!

Nessa topologia, um anel é relativamente fácil de ser instalado e reconfigurado, com isolamento de falhas simplificado. *Por que?* Porque para instalar, basta conectar os dispositivos e, caso uma nova máquina seja adicionada/eliminada, exige-se apenas a mudança de poucas conexões. Outra vantagem é o isolamento de falhas simplificado, isto é, se um dispositivo não receber o sinal de que os dados foram recebidos, ele pode emitir um alerta – facilitando a identificação do problema.

Por outro lado, há também desvantagens: se algum enlace for rompido, a rede inteira para de funcionar. Além disso, como o tráfego de dados é simplex, se alguma estação se tornar inoperante por alguma razão, a rede também para de funcionar. Existem também uma limitação quanto ao comprimento máximo do anel e o número máximo de dispositivos. *Como*

assim? Em um anel com 100 máquinas, por exemplo, o atraso para recebimento dos dados seria enorme.

Existiram implementações dessa tecnologia que utiliza anéis duplos para mitigar grande parte desses riscos e desvantagens (Ex: FDDI).

#VamosPraticar#

(QUADRIX / CRECI-PR – 2023) Na topologia em anel de uma rede de computadores, todos os dispositivos (computadores) estão conectados a um hub central.

Comentários: na topologia em anel de uma rede de computadores, os dispositivos não estão conectados a um hub central. Na verdade, cada dispositivo está conectado diretamente ao dispositivo vizinho, formando um circuito fechado, seja fisicamente (anel físico) ou logicamente (anel lógico). Não há um hub central na topologia em anel; em vez disso, os dispositivos são conectados em série, e a comunicação ocorre passando de um dispositivo para o próximo até chegar ao destino (Errado).

#VamosPraticar#

Questão

2022

4001329576

Nos itens que avaliem conhecimentos de informática, a menos que seja explicitamente informado o contrário, considere que: todos os programas mencionados estejam em configuração-padrão, em português; o mouse esteja configurado para pessoas da direita; expressões como **clique**, **clique simples** e **clique duplo** referem-se a cliques com o botão esquerdo do mouse; e **teclar** corresponda à operação de pressionar uma tecla e, rapidamente, liberá-la, acionando-a apenas uma vez. Considere também que não haja restrições de proteção, de funcionamento e de uso em relação aos programas, arquivos, diretórios, recursos e equipamentos mencionados.

Acerca dos conceitos de hardware, dos conceitos de redes de computadores e do programa de correio eletrônico Microsoft Outlook, versão web, julgue o item de 34.

Na topologia em anel, a comunicação entre os nós da rede somente pode ser realizada no sentido horário.

Solução

Gabarito: Errado.

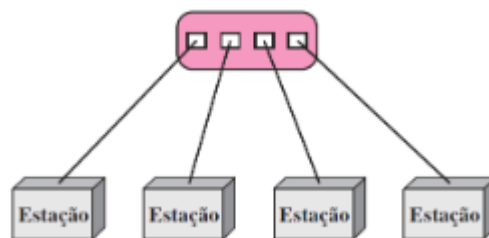
na topologia em anel, a comunicação entre os nós da rede pode ocorrer em ambas as direções: sentido horário e sentido anti-horário (Errado).

Estrela (Star)

INCIDÊNCIA EM PROVA: Altíssima

Nessa topologia, as estações são ligadas através de uma conexão ponto-a-ponto dedicada a um nó central controlador, ^[5] pelo qual passam todas as mensagens, não admitindo tráfego direto entre os dispositivos. Notem que eu disse que o enlace entre estações e o nó central é ponto-a-ponto e, não, que a arquitetura de rede é ponto-a-ponto. Não confundam! Cada dispositivo se conecta ao nó central por meio de um link dedicado, portanto usa um tipo de enlace ponto-a-ponto.

Trata-se da topologia mais utilizada atualmente por facilitar a adição de novas estações de trabalho e pela fácil identificação ou isolamento de falhas. No primeiro caso, para adicionar ou remover uma nova estação de trabalho, basta conectá-la ou desconectá-la da porta do nó central. No segundo caso, caso um cabo venha a se romper, não afetará as outras estações – afetará apenas a estação conectada por esse cabo. Logo, torna-se fácil identificar e isolar as falhas.



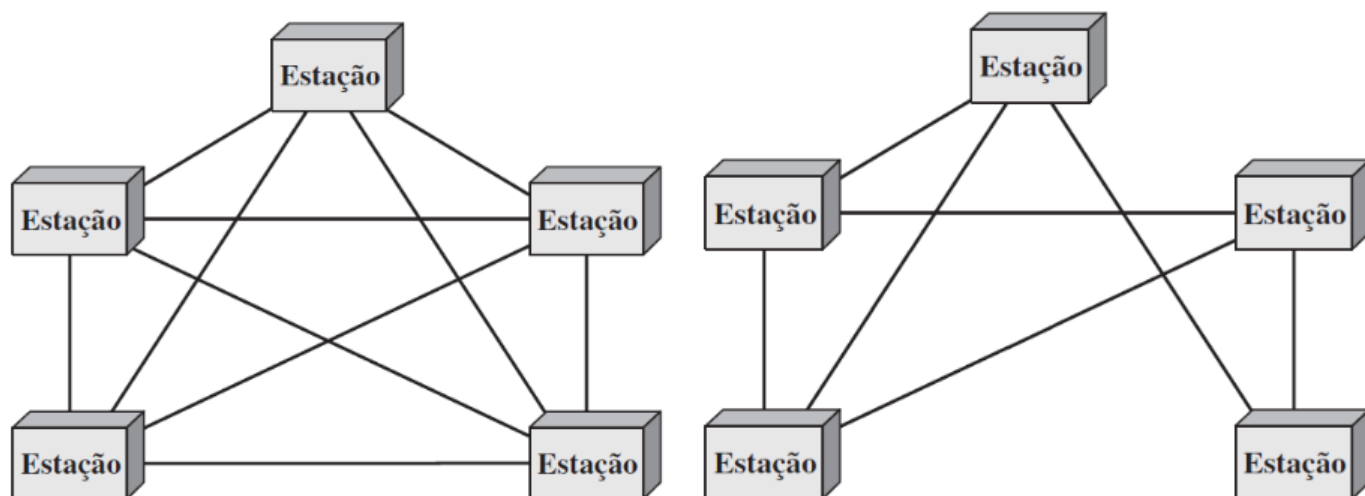
Observem que para que uma estação de trabalho envie uma informação para outra, haverá sempre uma passagem pelo nó central. Aliás, essa é uma das desvantagens dessa topologia: existe um ponto único de falha, isto é, se o dispositivo central falhar, toda a rede será prejudicada. Para reduzir essa probabilidade, utilizam-se dispositivos redundantes para que, caso algum pare de funcionar, o outro entra em ação.

Malha (Mesh)

INCIDÊNCIA EM PROVA: baixa

Nessa topologia, cada estação de trabalho possui uma conexão ponto a ponto direta e dedicada entre as demais estações da rede, de modo que não exista uma hierarquia entre elas. Nas imagens seguintes, temos dois exemplos de Topologia em Malha: à esquerda, temos

uma malha completa (também chamada de *Full Mesh*), isto é, cada nó se conecta a todos os outros nós; à direita, temos uma malha parcial, isto é, nem todos os nós se conectam aos outros nós [6].



Uma topologia em malha oferece várias vantagens em relação às demais topologias de rede. **Em primeiro lugar, o uso de links dedicados garante que cada conexão seja capaz de transportar seu próprio volume de dados, eliminando, portanto, os problemas de tráfego que possam ocorrer quando os links tiverem de ser compartilhados por vários dispositivos.** Em segundo, uma topologia de malha é robusta.

Se um link se tornar-se inutilizável, ele não afeta o sistema como um todo. O terceiro ponto é que há uma vantagem de privacidade e segurança. Quando qualquer mensagem trafega ao longo de uma linha dedicada, apenas o receptor pretendido a vê. Os limites físicos impedem que outros usuários acessem essa mensagem. **Finalmente, os links ponto a ponto facilitam a identificação de falhas, bem como o isolamento destas.**

O tráfego pode ser direcionado de forma a evitar links com suspeita de problemas. Essa facilidade permite ao administrador de redes descobrir a localização exata da falha e ajuda na descoberta de sua causa e solução. *E as desvantagens, Diego?* **As principais desvantagens de uma topologia em malha estão relacionadas à escalabilidade e ao custo, isto é, crescimento da quantidade de cabeamento e o número de portas necessárias para sua implementação.**

Em primeiro lugar, como cada dispositivo tem de estar conectado a cada um dos demais, a instalação e a reconstrução são trabalhosas. Em segundo, o volume de cabos pode ser maior que o espaço disponível seja capaz de acomodar (nas paredes, tetos ou pisos). Finalmente, o hardware necessário para conectar cada link (portas, placas e/ou cabos) pode ter um custo proibitivo. **Por tais razões, uma topologia de malha normalmente é implementada de forma limitada.**

Em outras palavras, essa topologia é mais adequada para poucas máquinas, caso contrário sua implementação pode se tornar inviável. Pensa comigo: se um computador estiver ligado

diretamente a outros quatro, nós precisaremos de 20 portas ou placas de rede e 10 cabos. Na verdade, para cada n computadores, são necessário $n.(n-1)/2$ cabos e $n.(n-1)$ portas ou placas de rede. Para 20 computadores, seriam 190 cabos e 380 placas de rede! 🤖

A utilização mais comum desse tipo de rede é para interligar – por exemplo – matrizes e filiais em uma rede metropolitana cabeada. Galera, na prática quase ninguém usa topologia em malha em Redes LAN (cabeadas): ou ela é utilizada em Redes WAN ou é utilizada em Redes WLAN (não cabeadas). Aliás, esse último caso tem sido cada vez mais comum: a topologia em *mesh* são comumente utilizadas em redes locais *wireless* para interligar dispositivos sem fio.

Talvez vocês já tenham visto que recentemente aumentou o número de vendas de kits de **roteadores *mesh* capazes de criar uma rede em malha em casas ou escritórios**. Um exemplo:



Eles são muito úteis para cobrir uma área grande com wi-fi. Sabe aquele ponto da casa que o sinal de wi-fi é ruim? Pois é, ele ajuda a melhorar esse sinal! Professor, não basta comprar um roteador e dois repetidores – que são bem mais baratos? Você pode fazer isso, mas você criará três redes diferentes e sempre que você quiser ter o melhor sinal possível, você terá que acessar o seu dispositivo, ir até as configurações e trocar de rede.

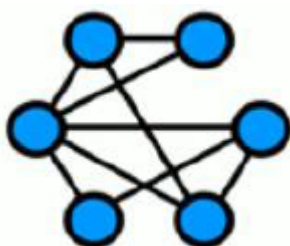
Na prática, sempre que você se mover pela casa ou escritório, você terá que ir trocando de rede para ter o melhor sinal possível. Já em redes *mesh*, isso não é necessário: **ela identifica onde está o nó com o sinal mais forte e se conecta automaticamente à medida que você vai se movendo pela casa.** E essa é apenas uma das vantagens! Enfim... trata-se de um belo investimento para quem tem problema de sinal.

Agora para finalizar essa parte de classificação de redes de computadores, eu fiz a tabelinha seguinte: ela mostra a relação entre topologia física, direção/modo de transmissão e tipo de enlace:

TOPOLOGIA física	DIREÇÃO DE TRANSMISSÃO	Tipo de ENLACE	MODOS DE TRANSMISSÃO
Barramento	Half-Duplex	Multiponto	Broadcast
Anel	Simplex	Ponto-a-Ponto	Broadcast
Estrela	Half-Duplex, se usar Hub; caso contrário Full-Duplex	Ponto-a-Ponto	Broadcast, se usar Hub; caso contrário, Unicast, Multicast ou Broadcast
Malha	Depende	Ponto-a-Ponto	Unicast, Multicast ou Broadcast

#VamosPraticar#

(IBADE / Prefeitura de Acrelândia-AC – 2022) Com relação às topologias de rede, analise a imagem abaixo e responda corretamente.



A topologia representada na imagem acima é a:

- a) barramento.
- b) mista.
- c) malha.
- d) árvore.
- e) estrela.

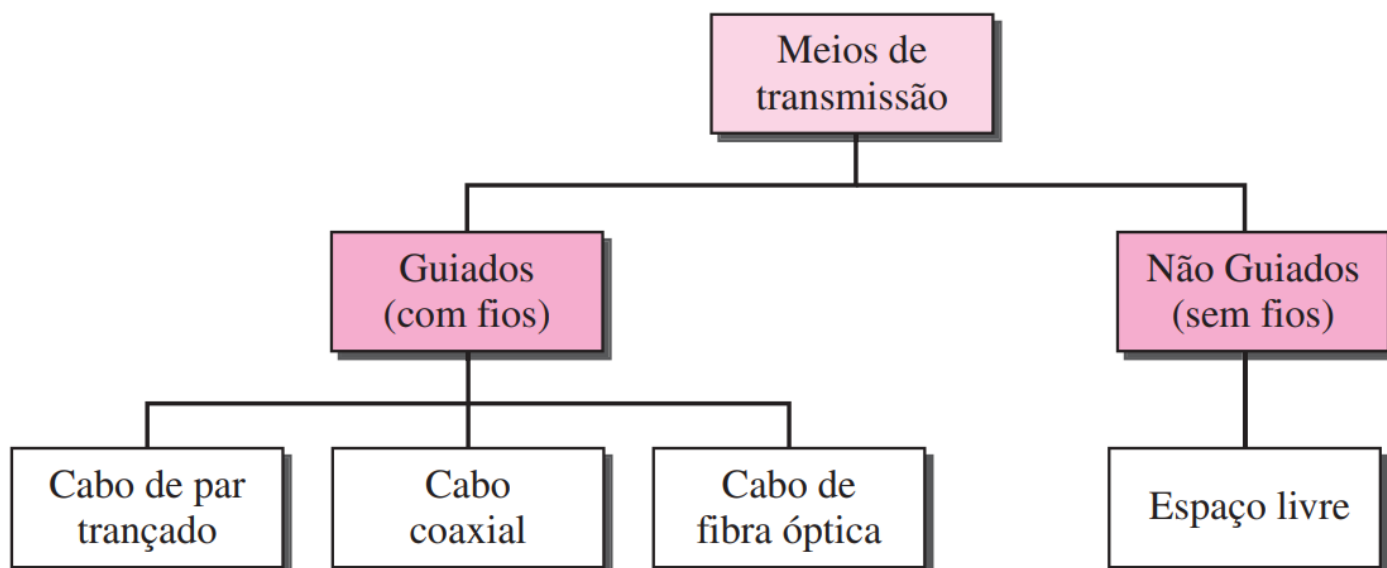
Comentários: a topologia apresentada é uma topologia em malha. Note que ela é caracterizada por um layout de rede em que os dispositivos estão interconectados, criando uma rede altamente redundante. Em uma topologia em malha, cada dispositivo é conectado diretamente aos outros dispositivos, formando uma teia de conexões e não há um único ponto central como em uma topologia em estrela (Letra C).

#VamosPraticar#

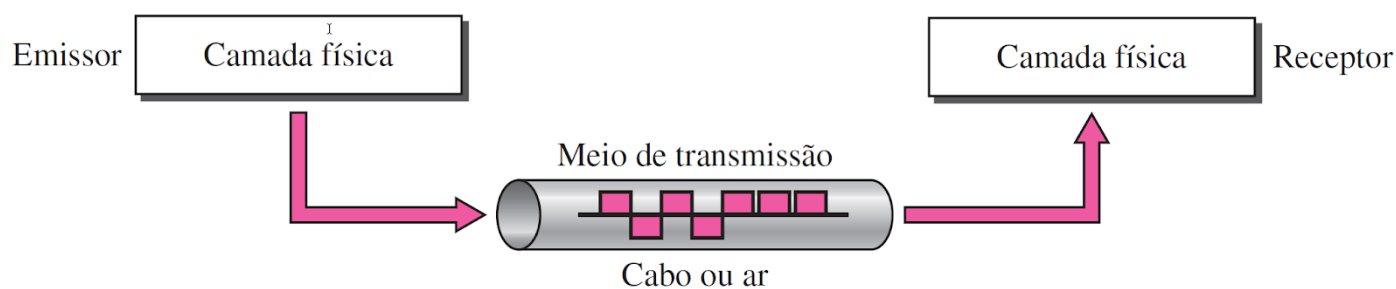
1.6 Redes de Computadores - Parte 1 - Meios de Transmissão - Teoria

Meios de Transmissão

Um meio de transmissão, em termos gerais, pode ser definido como qualquer coisa capaz de transportar informações de uma origem a um destino. Por exemplo: o meio de transmissão para duas pessoas conversando durante um jantar é o ar; para uma mensagem escrita, o meio de transmissão poderia ser um carteiro, um caminhão ou um avião. **Em telecomunicações, meios de transmissão são divididos em duas categorias: meios guiados e não-guiados.**



TIPO DE MEIO	DESCRIÇÃO
GUIADO	Trata-se da transmissão por cabos ou fios de cobre, onde os dados transmitidos são convertidos em sinais elétricos que propagam pelo material condutor. Exemplo: cabos coaxiais, cabos de par traçado, fibra óptica, entre outros.
NÃO-GUIADO	Trata-se da transmissão por irradiação eletromagnética, onde os dados transmitidos são irradiados através de antenas para o ambiente. Exemplo: ondas de rádio, infravermelho, microondas, bluetooth e wireless.



#VamosPraticar#

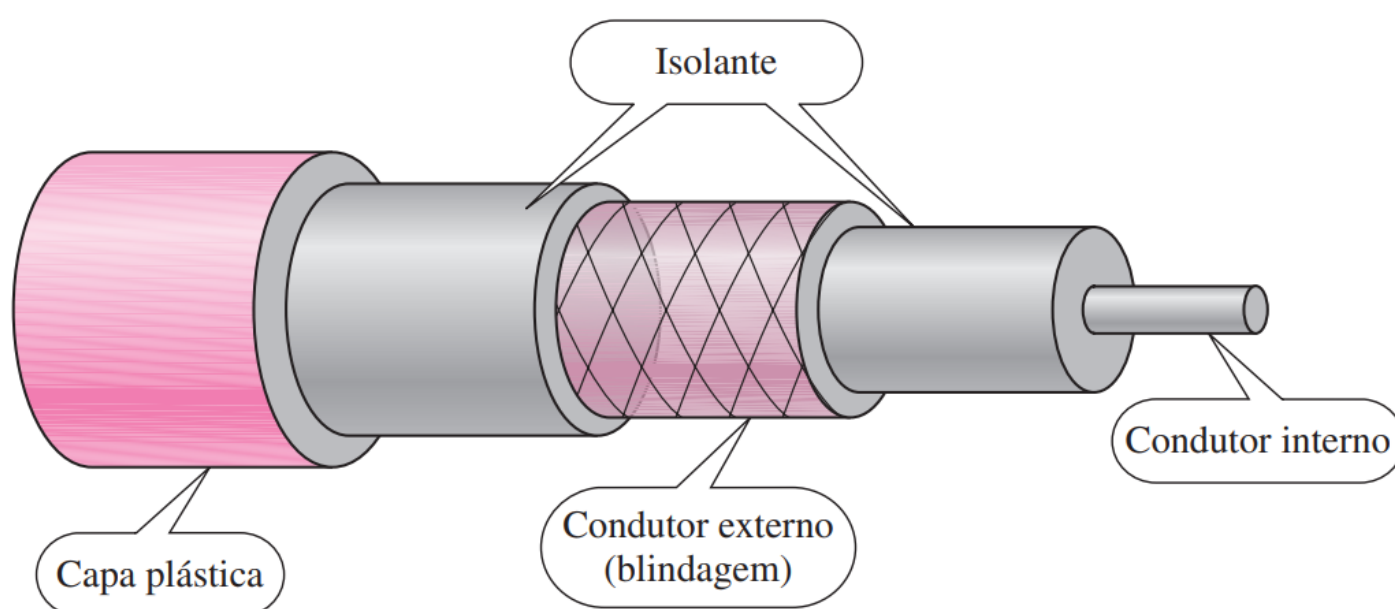
(QUADRIX / CRC-MG – 2022) O cabo UTP e as fibras ópticas são exemplos de meios de transmissão não guiados em uma rede de computadores.

Comentários: na verdade, ambos são considerados meios guiados em uma rede de computadores (Errado).

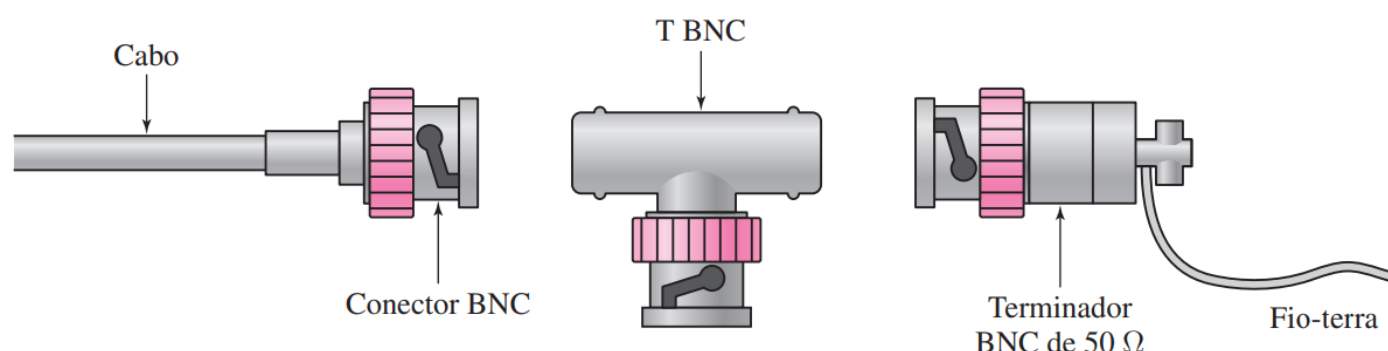
#VamosPraticar#

Cabo Coaxial

INCIDÊNCIA EM PROVA: baixa



Consiste em um fio central de cobre, envolvido por uma blindagem metálica. Isolantes de plástico flexível separam os condutores internos e externos e outras camadas do revestimento que cobrem a malha externa. Esse meio de transmissão é mais barato, pouco flexível e muito resistente à interferência eletromagnéticas graças a sua malha de proteção. Ele cobre distâncias maiores que o cabo de par trançado e utiliza um conector chamado **BNC** [7].



Foi utilizado até meados da década de 90 em redes de computadores, quando começou a ser substituído pelo cabo de par trançado. Ele ainda é utilizado em telecomunicações, basta dar uma olhadinha no decodificador da sua TV por Assinatura. **O cabo que chega na sua casa/prédio e que entra em um modem é geralmente um cabo coaxial** – ele é capaz de transportar sinais de Internet e TV.



Hoje em dia, provedores de TV/Internet têm substituído boa parte da mídia por cabos de fibra óptica. **Informação importante:** embora o cabo coaxial tenha uma largura de banda muito maior e cubra maiores distâncias que o cabo de par trançado, a sua taxa de transmissão é menor, o sinal se enfraquece mais rapidamente e ele requer o uso frequente de repetidores. É importante saber essas diferenças...

#VamosPraticar#

(PROF. DIEGO / INÉDITA – 2023) Cabos coaxiais são mais finos e flexíveis em comparação com cabos de fibra óptica.

Comentários: em comparação com cabos de par trançado e cabos de fibra óptica, os cabos coaxiais tendem a ser mais espessos e menos flexíveis, o que pode dificultar a instalação em espaços apertados (Errado).

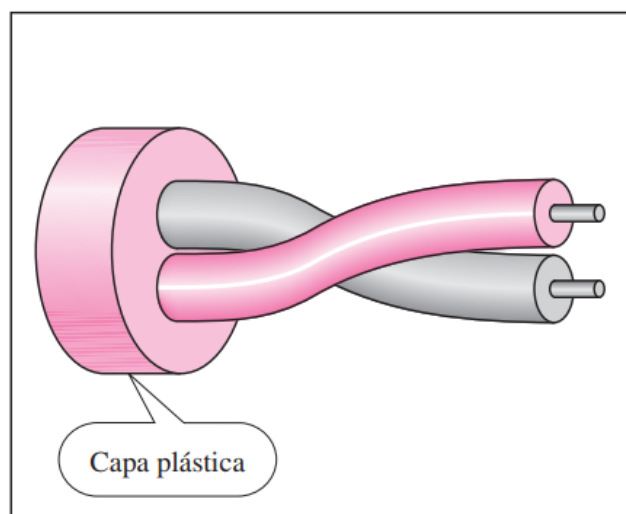
(PROF. DIEGO / INÉDITA – 2023) Cabos coaxiais geralmente usam conectores do tipo BNC (Bayonet Neill-Concelman) para estabelecer conexões.

Comentários: cabos coaxiais, de fato, frequentemente utilizam conectores do tipo BNC para fazer conexões seguras e estáveis (Correto).

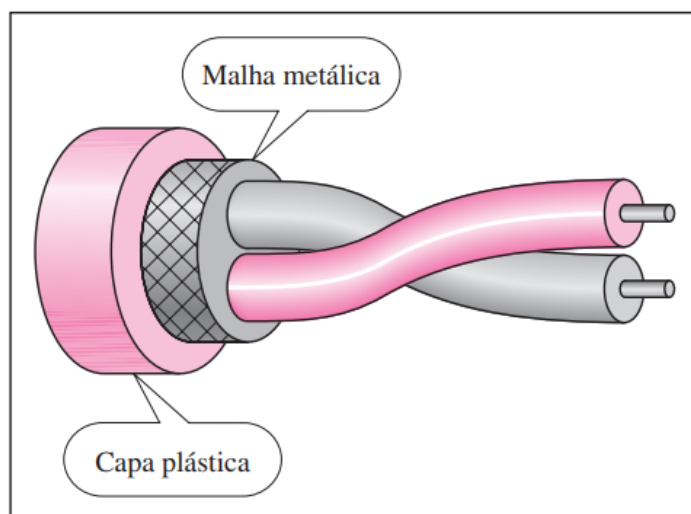
#VamosPraticar#

Cabo de Par Trançado

INCIDÊNCIA EM PROVA: ALTA

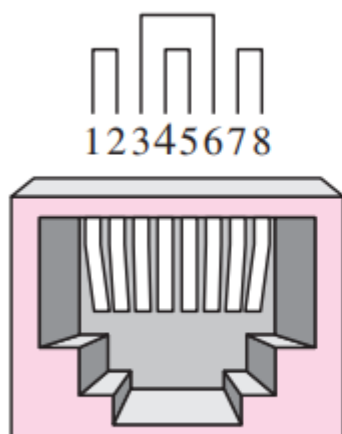


a. UTP

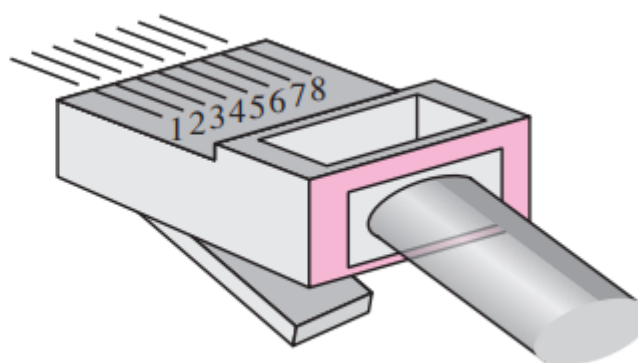


b. STP

Consiste em quatro pares de fios trançados blindados ou não, e envolto de um revestimento externo flexível. Eles são trançados para diminuir a interferência eletromagnética externa e interna – quanto mais giros, maior a atenuação. Este é o cabo mais utilizado atualmente por ser o mais barato de todos e ser bastante flexível. Esse cabo cobre distâncias menores que o cabo coaxial e utiliza um conector chamado RJ-45 (**Memorizem!**).



RJ-45 Fêmea

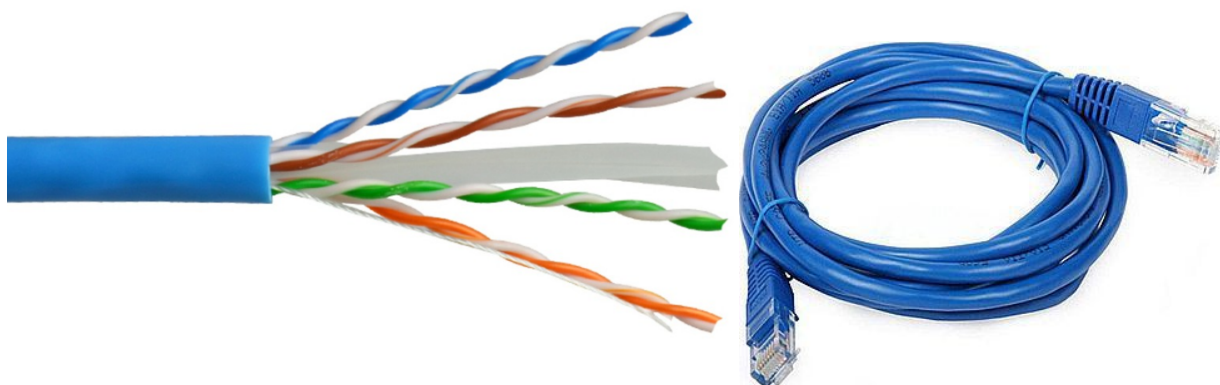


RJ-45 Macho

Quando é blindado, ele é chamado de Cabo STP (*Shielded Twisted Pair*) e quando não é blindado, ele é chamado de Cabo UTP (*Unshielded Twisted Pair*). **Galera, esse é aquele cabinho azul que fica atrás do seu computador ligado provavelmente a um roteador.** Sabe aquele cabo do telefone fixo da sua casa? Ele é mais fininho, mas ele também é um cabo de par trançado. Comparado ao cabo coaxial, tem largura de banda menor, mas taxas de transmissão maiores. Vejamos suas categorias:

CATEGORIA	taxa máxima de transmissão	Largura de banda	DISTÂNCIA MÁXIMA
-----------	----------------------------	------------------	------------------

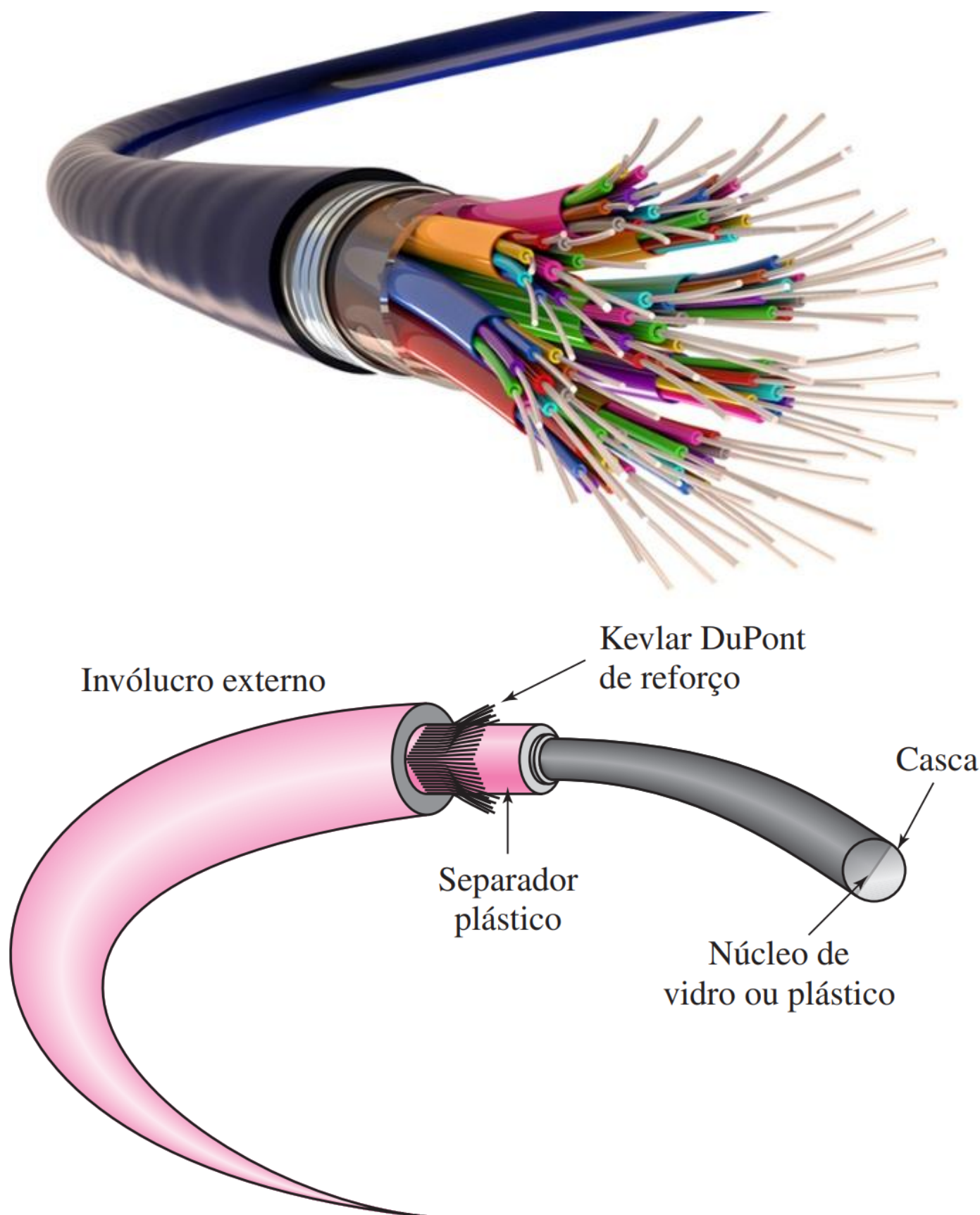
CAT3	Até 10 MBPS	16 MHz	100 Metros
CAT4	Até 16 MBPS	20 MHz	100 Metros
CAT5	Até 100 MBPS	100 MHz	100 Metros
CAT5e	Até 1000 MBPS (1G)	100 MHz	100 Metros
CAT6	Até 10000 MBPS (10G)	250 MHz	100 Metros
CAT6A	Até 10000 MBPS (10G)	500 MHz	100 Metros
CAT7	Até 10000 MBPS (10G)	600 MHz	100 Metros
CAT7A	Até 10000 MBPS (10G)	1000 MHz	100 Metros
CAT8	Até 40000 MBPS (40G)	2000 MHz	100 Metros



Os cabos de par trançado possuem quatro pares de fios, sendo alguns utilizados para transmissão e outros para recepção, permitindo uma comunicação *full duplex*. Para facilitar a identificação, os pares são coloridos e a ordem dos fios dentro do conector é padronizada. Eles podem ser utilizados na transmissão de sinais analógicos ou digitais. E a largura de banda depende da espessura do fio e da distância percorrida.

Cabo de Fibra Óptica

INCIDÊNCIA EM PROVA: média



O cabo de fibra óptica consiste em uma casca e um núcleo (de vidro, mais comum; ou plástico) para transmissão de luz. Esse tipo de cabo é normalmente encontrado em backbones de redes por apresentar excelente relação entre ampla largura de banda e custo.

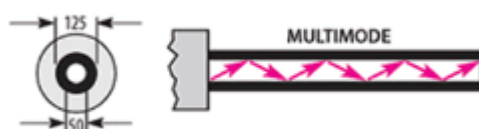
Hoje em dia, podemos transferir dados à velocidade de até 1.600 Gbps. Vejamos algumas vantagens e desvantagens dessa tecnologia:

VANTAGENS	DESCRIÇÃO
LARGURA DE BANDA MAIS AMPLA	Pode suportar larguras de banda muito maiores (e, consequentemente, maiores velocidades) que o cabo de par trançado ou coaxial. Atualmente, as taxas de dados e a utilização de largura de banda não são limitadas pelo meio de transmissão, mas sim pelas tecnologias de geração e recepção de sinais disponíveis.
MENOR ATENUAÇÃO DO SINAL	A distância de transmissão por fibra óptica é significativamente maior que a de qualquer outro meio de transmissão guiado. Um sinal pode percorrer 50 km sem precisar de regeneração. No caso de cabos coaxiais ou de par trançado, precisamos de repetidores a cada 5 km.
IMUNIDADE À INTERFERÊNCIA ELETROMAGNÉTICA	Ruídos eletromagnéticos não são capazes de afetar os cabos de fibra óptica.
RESISTÊNCIA A MATERIAIS CORROSIVOS e peso leve	O vidro é mais resistente a materiais corrosivos que o cobre. Além disso, os cabos de fibra óptica são muito mais leves que os cabos de cobre.
Maior imunidade à interceptação	Os cabos de fibra óptica são mais imunes à interceptação que os cabos de cobre. Os cabos de cobre criam efeitos antena que podem ser facilmente interceptados.

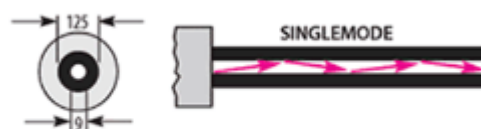
DESVANTAGENS	DESCRIÇÃO
INSTALAÇÃO E MANUTENÇÃO	O cabo de fibra óptica é uma tecnologia relativamente nova. Sua instalação e sua manutenção exigem mão-de-obra especializada, que não se encontra com facilidade.

PROPAGAÇÃO UNIDIRECIONAL DA LUZ	A propagação da luz é unidirecional. Se precisarmos de comunicação bidirecional, serão necessários dois cabos de fibra óptica.
CUSTO	O cabo e as interfaces são relativamente mais caros que outros meios de transmissão guiados. Se a demanda por largura de banda não for alta, muitas vezes o uso de fibra óptica não pode ser justificado.

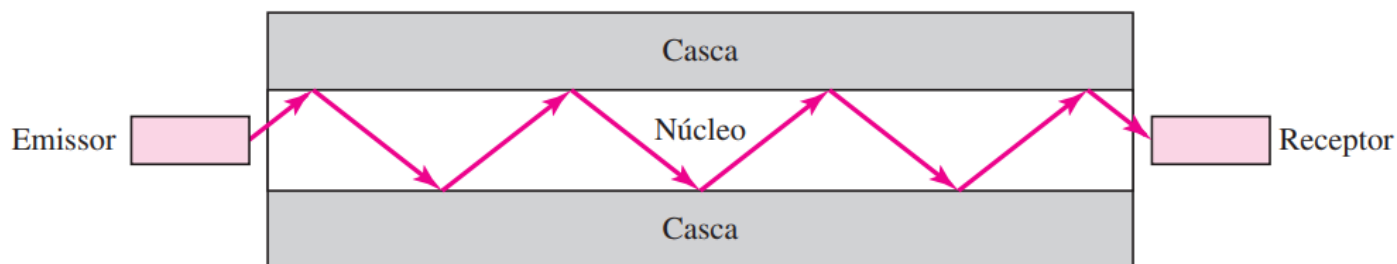
A tecnologia atual suporta dois modos para propagação da luz ao longo de canais ópticos, cada um dos quais exigindo fibras ópticas com características físicas diferentes: **Monomodo e Multimodo**.



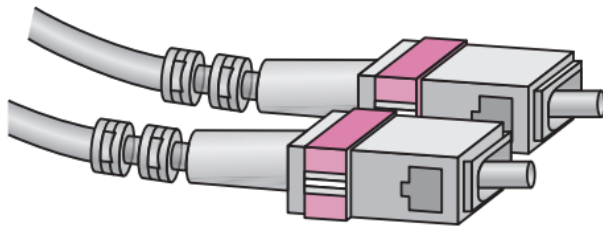
A Fibra Multimodo leva o feixe de luz **por vários modos ou caminhos**, por uma distância menor, com menores taxas de transmissão, mais imprecisa, diâmetro maior e alto índice de refração e atenuação, mas possui construção mais simples, é mais barata e utilizada em LANs.



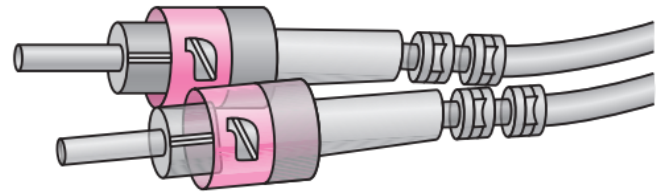
A Fibra Monomodo leva o feixe de luz **por um único modo ou caminho**, por uma distância maior, com maiores taxas de transmissão, mais precisa, diâmetro menor e baixo índice de refração e atenuação, mas possui construção mais complexa, é mais cara e utilizada em WANs.



Para fibras ópticas, existem dezenas de conectores diferentes no mercado, mas os mais comuns são os conectores ST (Straight Tip) e SC (Subscriber Connector). **Outra observação: antigamente uma fibra óptica era capaz de enviar dados em apenas uma direção (simplex). Atualmente ela já permite a comunicação bidirecional, isto é, são capazes de enviar dados em ambas as direções (full-duplex).**



Conector SC



Conector ST

#VamosPraticar#

(QUADRIX / CRMV-MS – 2022) A fibra óptica, devido à sua alta taxa de interferência, não pode ser utilizada em redes MAN (Metropolitan Area Network).

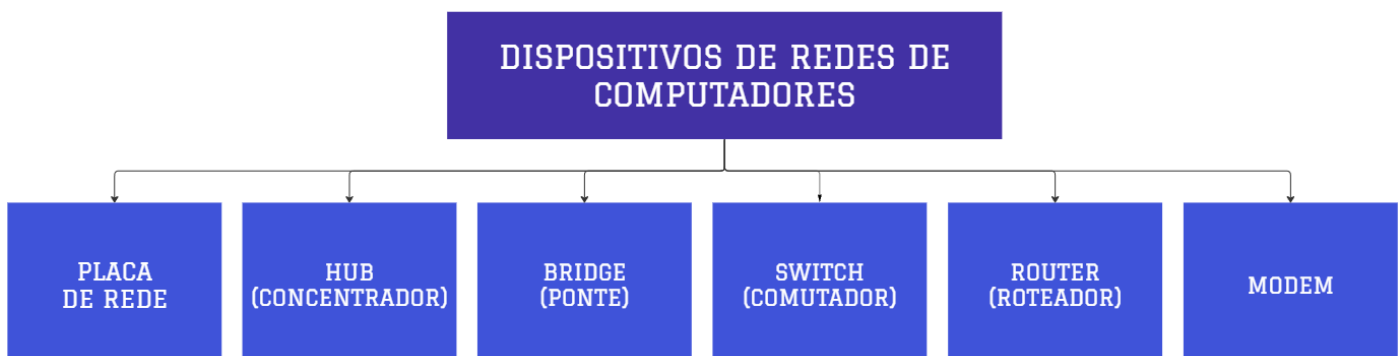
Comentários: a fibra óptica é uma escolha comum e altamente eficiente em redes MAN (Metropolitan Area Network). Ela é frequentemente usada para transmitir dados em distâncias metropolitanas, devido à sua capacidade de alta largura de banda e imunidade a interferências eletromagnéticas (Errado).

#VamosPraticar#

1.7 Redes de Computadores - Parte 1 - Equipamentos de Redes - Teoria

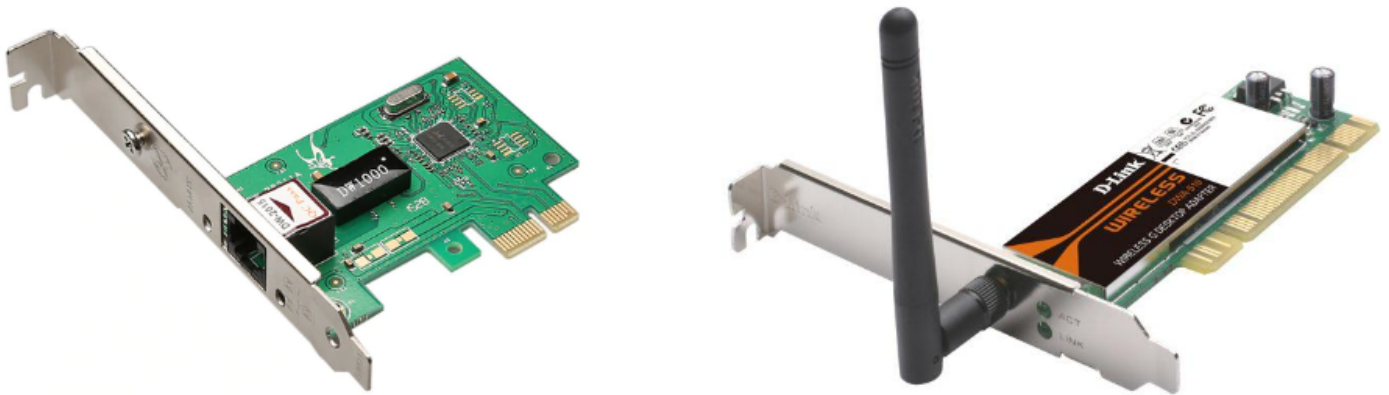
Equipamentos de Redes

Galera, os equipamentos ou dispositivos de uma rede podem classificados como finais ou intermediários. No primeiro caso, trata-se daqueles dispositivos que permitem a entrada e/ou saída de dados (Ex: Computador, Impressora; Câmeras, Sensores, etc); no segundo caso, trata-se daqueles que compõem a infraestrutura de uma rede (Hub, Bridge, Switch, Router, etc). Nós vamos nos focar agora nos dispositivos intermediários. Venham comigo...



Network Interface Card (NIC ou Placa de Rede)

INCIDÊNCIA EM PROVA: baixíssima



Trata-se de um dispositivo eletrônico, interno ou externo a uma estação, contendo circuitos que permitem a uma estação se conectar a uma rede. Em outras palavras, trata-se de um hardware que permite que um computador se conecte a uma rede de computadores e se comunique com outros dispositivos na rede. Ela é responsável por fornecer uma interface entre o computador e o meio físico da rede (de forma cabeada ou não).

Essas são as famosas Placas de Rede – também chamada de Placas NIC. Na imagem apresentada à esquerda, temos uma placa de rede cabeada e, na imagem apresentada à direita, temos uma placa de rede não cabeada (*wireless*). Essas placas podem ser instaladas internamente em um computador (forma mais comum) ou podem ser dispositivos externos, como pequenos adaptadores USB.

Se vocês olharem na parte de trás do gabinete de um computador, vocês poderão vê-las (provavelmente com o cabo de par trançado conectado a ela). Elas permitem uma comunicação bidirecional – transmissão e recebimento de dados – com os demais elementos da rede. **Essas placas são essenciais para que um computador acesse uma rede local ou a internet – sendo amplamente utilizadas em desktops, notebooks, servidores e outros dispositivos de rede.**

As placas de rede podem oferecer suporte a diferentes tipos de conexões de rede, como Ethernet, Wi-Fi, entre outros. Elas são responsáveis por converter os dados do computador em sinais que podem ser transmitidos pela rede e também por receber sinais da rede e entregá-los ao sistema do computador. **Agora um ponto importante: placas de rede possui um identificador único e exclusivo chamado Endereço MAC (Media Access Control).**

Esse endereço é gravado na fábrica e não pode ser alterado, a menos que seja um processo excepcional. O endereço MAC é composto por uma sequência de 12 dígitos hexadecimais (portanto, 48 bits). Ele é usado para identificar de forma única dispositivos em uma rede local.

Cada fabricante de dispositivos de rede é atribuído a um conjunto exclusivo de endereços MAC, garantindo que não haja conflitos de identificação em escala global.

Esse endereço desempenha um papel fundamental na comunicação de dados em uma rede, uma vez que é utilizado para rotear pacotes de dados para os dispositivos corretos na rede. Isso ajuda os dispositivos na mesma rede a se comunicarem entre si e garante que os dados sejam entregues ao destinatário adequado. Vejam a seguir um exemplo de endereço MAC (note que ele vem separado por dois-pontos).

00:1C:B3:09:85:15

CARACTERÍSTICA	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo que permite que um computador se conecte a uma rede de computadores, seja por meio de cabo ou sem fio.
CAMADA OSI	Camada 2 (Enlace). Atenção: vamos estudar o que são as camadas OSI mais à frente.
VANTAGENS	Permite que um computador se conecte a redes locais e à internet; facilita a comunicação entre dispositivos em uma rede; e oferece a capacidade de transmissão e recepção de dados.
DESVANTAGENS	Em redes sem fio, a qualidade do sinal pode afetar o desempenho; e pode ser uma vulnerabilidade de segurança se não configurada corretamente.

#VamosPraticar#

(PROF. DIEGO / INÉDITA – 2023) Uma placa de rede não é necessária em um computador para conexão com a Internet, pois os modems modernos desempenham essa função.

Comentários: uma placa de rede é necessária para conectar o computador à rede local, e muitos modems modernos têm uma placa de rede embutida para conectar o computador à Internet (Errado).

(PROF. DIEGO / INÉDITA – 2023) Placas de rede são adequadas apenas para redes com fio e não podem ser usadas em redes sem fio (Wi-Fi).

Comentários: placas de rede Ethernet são projetadas para redes com fio e usam cabos para conexão. Para redes sem fio, são necessárias placas de rede Wi-Fi (Correto).

(QUADRIX / CRO-SC – 2023) A placa de rede, ou adaptador de rede, é o dispositivo de hardware utilizado para que um computador se conecte a uma rede de computadores; esse dispositivo possui um número único de identificação, chamado endereço IP.

Comentários: a placa de rede, ou adaptador de rede, é, de fato, um dispositivo de hardware utilizado para conectar um computador ou dispositivo a uma rede de computadores. No entanto, ela é identificada pelo seu endereço MAC (Media Access Control), que é um número único atribuído a cada placa de rede. Não é o endereço IP, mas o endereço MAC que serve como identificação exclusiva da placa de rede (Errado).

(QUADRIX / CRQ-MS – 2021) Assinale a alternativa que apresenta o nome do endereço físico, que é atribuído por seu fabricante, de uma placa de rede, seja ela para rede cabeada ou sem fio.

- a) endereço MAC
 - b) endereço IP
 - c) DHCP
 - d) DNS
 - e) UDP
-

Comentários: o endereço MAC é o endereço físico único atribuído por um fabricante a uma placa de rede. É usado para identificar exclusivamente uma placa de rede em uma rede local (Letra A).

(CESPE / APEX – 2021) Os computadores comunicam-se entre si e com os demais meios de transmissão de dados por meio de placas de rede, as quais possuem um número único denominado:

- a) Endereço WWW (World Wide Web).
- b) Endereço IP (Internet Protocol).
- c) Endereço MAC (Media Access Control).
- d) Endereço de email (correio eletrônico).

Comentários: o número único e exclusivo de placas de rede é o Endereço MAC (Letra C).

Hub (Concentrador)

INCIDÊNCIA EM PROVA: média



Inicialmente, é importante saber que existem hubs ativos e passivos. **Um hub passivo é simplesmente um conector que concentra e conecta os cabos provenientes de diferentes ramificações. Esse dispositivo sequer é conectado na rede elétrica, portanto não é capaz de regenerar sinais digitais.** Pessoal, se uma questão não mencionar o tipo de hub, podemos assumir que ela está tratando de hubs ativos. Vamos estudá-lo com um pouco mais de detalhes...

Um hub ativo é um dispositivo para interligação de computadores que tem o objetivo de concentrar os enlaces e aumentar o alcance de uma rede local por meio da regeneração de

sinais. Pessoal, sinais que transportam dados dentro de uma rede podem trafegar por uma distância fixa. Após essa distância, o sinal começa a se atenuar, colocando em risco a integridade dos dados (isto é, correndo risco de haver perda de dados).

Um hub ativo atua como repetidor, recebendo sinais digitais e, antes de se tornar muito fraco ou corrompido, regenerando-o para o seu padrão de bits original. O repetidor encaminha, então, o sinal regenerado. Pode-se afirmar, portanto, que ele pode estender o comprimento físico de uma rede local. **O hub ativo é considerado um repetidor multiportas porque ele regenera e transmite os sinais entre suas portas. Atualmente, esse equipamento está obsoleto.**

O Hub é considerado um dispositivo “burro” por trabalhar apenas com *broadcast*. *Como assim, professor?* **Ao receber dados, ele os distribui para todas as outras portas – ele não é capaz de transmitir dados somente para uma porta específica.** Dessa forma, apenas uma máquina pode transmitir dados de cada vez para evitar colisões, portanto ele trabalha com a direção de transmissão half-duplex.

Agora vamos ver se vocês entenderam mesmo o tópico de topologia de redes. Nós já sabemos que a topologia física trata de como estão dispostos os links (cabos) e os nós de uma rede. E sabemos que a topologia lógica trata de como os dados efetivamente percorrem os links e transitam entre dispositivos. Por outro lado, nós também sabemos que um hub ativo é responsável por concentrar os cabos em um único local e por trabalhar apenas em broadcast. Dito isso...

QUAL É A TOPOLOGIA FÍSICA

E LÓGICA DE UM HUB ATIVO?

Ora, se ele concentra todos os cabos, então sua topologia física é em estrela; e se ele somente trabalha em broadcast, isto é, os dados são transmitidos para todos os dispositivos, então sua topologia lógica é em barramento. **Em suma: o hub ativo é um equipamento de rede concentrador de enlaces que permite também concentrar o tráfego de rede que provém de vários dispositivos, assim como regenerar o sinal.**

O seu objetivo é recuperar os dados que chegam a uma porta e enviá-los para todas as demais portas. A representação de um Hub é apresentada abaixo:



CARACTERÍSTICA	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo que simplesmente repete os dados recebidos em uma porta para todas as outras portas (está em desuso atualmente).
CAMADA OSI	Camada 1 (Física).
VANTAGENS	Custo geralmente baixo; simplicidade de operação; adequado para redes muito pequenas.
DESVANTAGENS	Pode causar tráfego ineficiente e colisões de dados; pode levar à degradação do desempenho em redes maiores; não possui inteligência para direcionar pacotes apenas para o destino certo.

#VamosPraticar#

(QUADRIX / PRODAM – 2022) Assinale a alternativa correta referente aos hubs.

- a) Um hub pode ter, no máximo, oito portas.
- b) O hub pode ser utilizado no controle de tráfego de dados de várias redes.
- c) Diferentemente dos computadores, um hub não possui endereço IP, uma vez que ele não possui memória interna para armazená-lo.
- d) O hub, assim como outros concentradores, possui um software hub, que permite repassar vários pacotes de dados de uma só vez.
- e) Um hub não pode ser conectado a outro hub, o que representa uma desvantagem dele em relação ao switch.

Comentários: (a) Errado, hubs podem ter mais do que oito portas, e o número de portas varia de acordo com o modelo do hub; (b) Correto, ele realmente pode ser utilizado para controle de tráfego - Quando um computador ligado à rede transmite informações para o hub, é necessário que ele esteja desocupado, pois, caso contrário, o pacote de dados é retornado ao

computador requisitante com um pedido de espera, até que a transmissão de informações que está sendo realizada pelo hub termine; (c) Errado, ele realmente não tem endereço IP, mas não por conta de não possuir memória interna e, sim, porque eles trabalham em uma camada mais básica de comunicação; (d) Errado, hubs não possuem software avançado para repassar vários pacotes de dados de uma só vez. Eles simplesmente repetem os dados em todas as portas, o que não envolve um processo complexo de tomada de decisão ou "repasse" de pacotes; (e) Errado, eles podem – sim – ser conectados a outro hub (Errado).

(QUADRIX / CRMV-MS – 2022) Um hub simula o comportamento de um barramento, ou seja, quando uma estação transmite, a transmissão é recebida por uma porta do hub e retransmitida para as outras.

Comentários: um hub é um dispositivo que opera na camada física da rede e funciona de forma semelhante a um barramento. Quando uma estação conectada a um hub transmite dados, o hub recebe esses dados em uma porta e os retransmite para todas as outras portas. Isso significa que todos os dispositivos conectados ao hub recebem a transmissão, independentemente do destinatário final, o que pode levar a colisões de dados em redes maiores (Correto).

(IDIB / CREMERJ – 2019) A respeito dos equipamentos de interconexão utilizados em redes de computadores, marque a alternativa que indica CORRETAMENTE o nome do dispositivo que, com o passar do tempo, caiu em desuso pelo fato de não ser capaz de direcionar a transmissão de dados em uma rede, limitando-se a atuar como um simples repetidor.

a) Host. b) Router. c) Hub. d) Switch.

Comentários: o dispositivo em desuso incapaz de encaminhar dados porque só transmite em broadcast é o Hub (Letra C).

(CESPE / FUB – 2016) Caso algum cabo de um hub apresente problema, todos os cabos de rede a ele conectados devem ser substituídos, pois, dada a simplicidade de funcionamento do hub, não é possível identificar o cabo defeituoso.

Comentários: em uma rede em que todos os dispositivos estão conectados a um hub, não é necessário substituir todos os cabos se um cabo específico apresentar problemas. Se houver um problema em um cabo específico, você pode substituir apenas esse cabo defeituoso, sem a necessidade de substituir todos os cabos da rede. O hub não é capaz de identificar cabos defeituosos, mas isso não afeta a capacidade de substituir apenas o cabo com defeito (Errado).

(CESPE / SERPRO – 2010) Um hub é, em termos físicos, uma topologia em estrela, mas que pode ser caracterizado, em termos lógicos, como uma topologia em barramento.

Comentários: ele realmente possui topologia física em estrela e lógica em barramento (Correto).

(FCC / SEFAZ-PB – 2006) Dispositivo físico que tem por função básica apenas interligar os computadores de uma rede local. Recebe dados vindos de um computador e os transmite às outras máquinas. Conhece-se também por concentrador:

- a) o parser
- b) o hub
- c) o router
- d) a bridge
- e) o gateway

Comentários: dispositivo que tem por função **básica** interligar computadores de uma rede local é o Hub (Letra B).

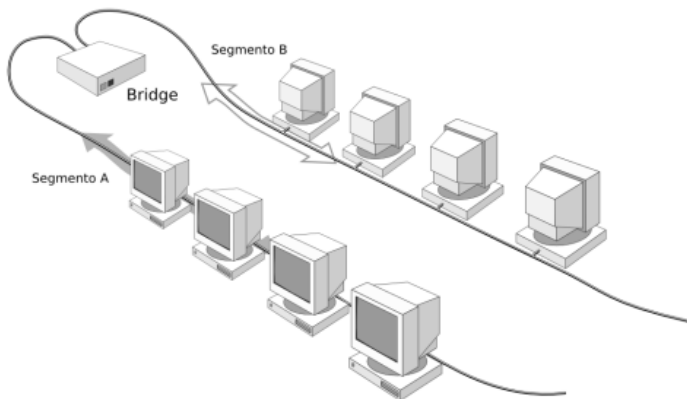
#VamosPraticar#

Bridge (Ponte)

INCIDÊNCIA EM PROVA: baixíssima

Uma bridge é um equipamento de rede que também é capaz de regenerar o sinal que recebe, porém ela tem uma função extra: possui capacidade de filtragem. *Como assim, Diego?* **Isso significa que ela é capaz de verificar o endereço de destino de um conjunto de dados e decidir se este deve ser encaminhado ou descartado.** Para tal, esse dispositivo possui uma tabela que associa endereços a portas, assim ela consegue decidir à quem os dados devem ser encaminhados.

Ela também permite conectar segmentos de redes que podem ou não utilizar tecnologias de enlace distintas (Ex: Ethernet + Token Ring) de forma que possam se comunicar como se fossem uma única rede. O que é um segmento de rede? É simplesmente subdivisão de uma rede. Vejam abaixo que uma rede foi separada em dois segmentos: Segmento A e Segmento B. Como a rede foi segmentada, nós temos uma redução no tráfego e uma menor chances de colisões.



Como assim uma redução no tráfego? Galera, os dados transmitidos para um segmento agora são enviados apenas para os computadores específicos e, não, para todos os computadores da rede – como ocorria com o hub! Lembrem-se que o hub envia dados para todos os computadores da rede indiscriminadamente. Logo, o tráfego na rede reduz e a chance de colisões também.

As informações manipuladas por uma bridge são chamadas de quadros ou frames – assim como no switch. Há diversos tipos de bridge: (1) simples – quando possui apenas duas portas, logo conecta apenas dois segmentos; (2) multiporta – quando possui diversas portas, logo conectam vários segmentos; (3) transparente – quando é invisível para outros dispositivos da rede, não necessitando de configurações; (4) de tradução – quando conecta redes de tecnologias de enlace diferentes.

Em suma: uma bridge é um equipamento de rede que permite conectar segmentos de rede diferentes que podem ou não utilizar tecnologias de enlace distintas de forma que sua agregação pareça uma única rede, permitindo filtrar os quadros para que somente passe para o outro segmento da bridge dados enviados para algum destinatário presente nele, e que permite a redução de tráfego de dados, o aumento da largura de banda e a separação dos domínios de colisão.

CARACTERÍSTICA	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo de rede utilizada para dividir uma rede em segmentos menores, reduzindo colisões e tráfego de rede desnecessário (está em desuso atualmente).
CAMADA OSI	Camada 2 (Enlace).
VANTAGENS	Filtra o tráfego, melhorando o desempenho; pode conectar diferentes tipos de redes (Ex: Ethernet e Wi-Fi); aumenta a segurança da rede, criando domínios de colisão separados.
DESVANTAGENS	Pode ser mais caro do que um hub simples; requer configuração e gerenciamento adequados; limitação da extensão da rede e a complexidade de gerenciamento em redes maiores.

#VamosPraticar#

(PROF. DIEGO / INÉDITA – 2023) Bridges ajudam a dividir uma rede em segmentos para reduzir o tráfego e melhorar o desempenho.

Comentários: as bridges segmentam redes em segmentos menores para limitar o tráfego e, assim, melhorar o desempenho (Correto).

(PROF. DIEGO / INÉDITA – 2023) As pontes são utilizadas – na grande maioria das vezes – para conectar redes com diferentes protocolos de comunicação.

Comentários: embora possam ser utilizadas para conectar redes com diferentes protocolos de comunicação, as pontes são mais frequentemente utilizadas para conectar segmentos de rede com o mesmo protocolo de comunicação, reduzindo o tráfego entre os segmentos (Errado).

(FUNDATEC / IFFAR – 2023) Qual o dispositivo de rede utilizado para juntar várias LANs físicas em uma única LAN lógica?

- a) Gateway.
- b) Roteador.
- c) Repetidor.
- d) Bridge.
- e) Hub.

Comentários: o dispositivo utilizado para juntar várias LANs físicas em uma única LAN lógica é a Bridge. Elas desempenham um papel importante na interconexão de redes locais, permitindo a comunicação entre diferentes segmentos de rede enquanto mantêm a segurança e o desempenho da rede (Letra D).

(CFM – 2018) Uma bridge é um mecanismo usado para conectar dois segmentos de rede diferentes e enviar quadros de um segmento ao outro de forma transparente.

Comentários: ela realmente conecta dois segmentos de rede diferentes e envia quadros (dados) de um segmento a outro. Transparente significa que não se enxerga! *Sabe quando você vai aos Correios e paga para entregar um pacote para alguém? Se o pacote vai de avião, navio ou carro não importa para você, logo o método de entrega é transparente (ele não enxerga o método). No caso da questão, a bridge envia quadros de um segmento ao outro de forma transparente, isto é, ela consegue enviar dados de um segmento para outro como se estivessem todos em um mesmo segmento sem problema algum visto que os dispositivos não têm conhecimento de sua existência (Correto).*

#VamosPraticar#

Switch (Comutador)

INCIDÊNCIA EM PROVA: média



Também conhecido como comutador, o switch é uma evolução dos hubs! **Eles são inteligentes, permitindo fechar canais exclusivos de comunicação entre a máquina que está enviando e a que está recebendo.** Em outras palavras, o switch é capaz de receber uma informação e enviá-la apenas ao seu destinatário. Ele não é como o hub, que recebia uma informação de fora e a repassava para todo mundo que estivesse na rede.

O hub é aquele seu amigo fofoqueiro que você pede para ele contar algo para outro amigo e ele sai contando para todo mundo. Já o switch é aquele amigo leal – se você pede para ele contar algo para outro amigo, ele conta apenas para esse amigo e, não, para os demais. **O nome dessa característica é encaminhamento ou filtragem, porque ele filtra as mensagens recebidas e encaminha apenas para o destinatário original.**

Outra característica importante desse equipamento é a **autonegociação**, isto é, a compatibilidade com diferentes Padrões Ethernet. Vamos ver padrões de redes em detalhes no próximo tópico, mas por enquanto basta saber que as tecnologias de padrões de rede vão evoluindo com o passar do tempo e passam a funcionar, por exemplo, com taxas de transmissão mais altas. *Como fazer para dois dispositivos com padrões diferentes conectados ao mesmo link possam conversar sem problemas?*

O recurso de autonegociação do switch permite que seja negociado tanto a taxa de transmissão de dados quanto a direção de transmissão, isto é, se um trabalha com uma taxa de transmissão maior e o outro com uma taxa de transmissão menor, eles negociam o envio de dados a uma taxa de transmissão menor de modo a manter uma compatibilidade e uma comunicação de dados eficiente e boa para todos.

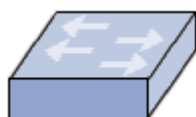
Outro recurso interessante é o autoaprendizado, ou seja, switches são equipamentos que não precisam ser configurados manualmente. *Como assim, Diego?* Quando você conecta um computador ao switch, você não precisa acessar o switch e informá-lo que o computador com endereço X está localizado na porta Y. O switch possui uma tabela dinâmica que automaticamente associa endereços aos computadores conectados.

A segmentação realizada pelo dispositivo possibilita que diferentes pares possam conversar simultaneamente na rede, sem colisões. A transmissão para canais específicos faz com que uma rede com switch possua topologia física e lógica em estrela. **Além disso, o Hub funciona apenas em half-duplex e o Switch em full-duplex. Dessa forma, a rede fica menos**

congestionada com o fluxo de informações e é possível estabelecer uma série de conexões paralelas.

Por fim, é importante tomar cuidado com a utilização do termo switch, visto que pode significar coisas distintas. Existe Switch de Camada 2 ou Switch de Camada 3. *Que camada é essa, professor?* Um Switch de Camada 3 é utilizado na camada de rede funcionando de forma mais similar a um roteador; e um Switch de Camada 2 opera nas camadas física e de enlace. Veremos essas camadas na próxima aula. **Se a questão não especificar, considere se tratar do Switch de Camada 2.**

Em suma: um switch (comutador) é um equipamento de rede semelhante a uma **ponte com múltiplas portas, capaz de analisar dados que chegam em suas portas de entrada e filtrá-los para repassar apenas às portas específicas de destino**. Além disso, ele tem recursos como autonegociação e autoaprendizagem, sendo capaz de funcionar em *full duplex* [8]. A representação de um Switch é abaixo:



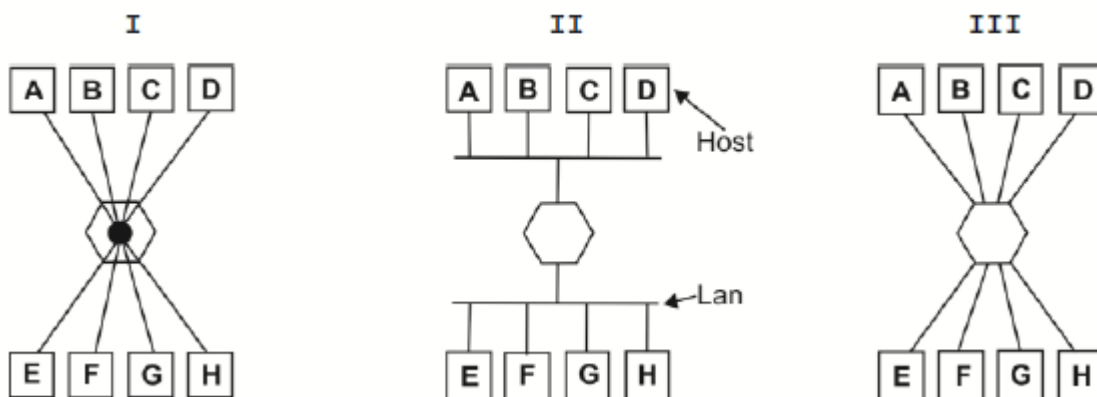
CARACTERÍSTICA	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo de rede projetado para encaminhar pacotes de dados com base nos Endereços MAC (Media Access Control).
CAMADA OSI	Camada 2 (Enlace).
VANTAGENS	Rápido encaminhamento de pacotes; reduz colisões na rede; segmenta o tráfego da rede em diferentes portas; suporta redes com fio e sem fio; melhora o desempenho da rede.
DESVANTAGENS	Mais caro do que um hub; requer configuração e gerenciamento adequados; pode ter uma curva de aprendizado para administradores de rede.

#VamosPraticar#

(QUADRIX / CRO-SC – 2023) O switch é um dispositivo de rede que roteia pacotes entre redes de computadores.

Comentários: o switch não roteia pacotes entre redes de computadores – ele opera em um nível mais baixo do modelo OSI, especificamente na camada de enlace de dados – o dispositivo de rede responsável por rotear pacotes é o roteador (Errado).

(FCC / TRT19 – 2022) As figuras a seguir mostram configurações de interconexão de computadores, representados pelas letras de A até H, em rede.



Observando as configurações I, II e III, um Analista classificou-as, correta e respectivamente, como:

- a) bridge gateway e switch.
- b) hub, roteador e gateway.
- c) repetidor, switch e roteador.
- d) gateway, repetidor e switch.
- e) hub, bridge e switch.

Comentários: (I) o primeiro dispositivo é um hub, dado que todas as mensagens são transmitidas para todos os demais dispositivos – é possível ver pelo desenho no centro do hub; (II) o segundo dispositivo é uma bridge, dado que interconecta dois segmentos de rede diferentes; (III) o terceiro dispositivo é um switch – ele se parece bastante com o hub pela imagem, mas percebe que as mensagens não são transmitidas para todos os dispositivos da

rede. Os desenhos poderiam ser melhores na questão para facilitar a diferenciação dos dispositivos (Letra E).

(SELECON / Prefeitura de Cuiabá-MT – 2018) Tendo por foco o modelo OSI/ISO, um equipamento de interconexão de nível 2 opera por meio da segmentação como comutador de rede na camada de enlace, além de representar um dispositivo para solucionar problemas de congestionamento. Esse equipamento é conhecido por:

a) hub b) router c) gateway d) switch

Comentários: nível 2, segmentação de redes, comutador, camada de enlace são todas palavras-chave para Switch (Letra D).

(IBFC / Prefeitura de Araraquara-SP – 2017) Em uma rede de computadores, que é utilizada a topologia em estrela, existe a necessidade de se utilizar o equipamento de rede denominado em inglês como:

a) gateway b) switch c) modem d) bridge

Comentários: (a) Errado. Um gateway é um dispositivo que atua como um ponto de entrada para outra rede. Embora seja um componente importante em redes, não é especificamente relacionado à topologia em estrela; (b) Correto. O switch é um dispositivo de rede que encaminha dados apenas para o dispositivo específico ao qual eles são destinados em uma rede local. É comumente usado em topologias em estrela para conectar vários dispositivos a um ponto central; (c) Errado. Um modem é um dispositivo que converte os sinais digitais de um computador em sinais analógicos para transmissão através de linhas de comunicação, como linhas telefônicas. Não é exclusivamente usado em topologias de estrela, mas pode ser encontrado em várias configurações de rede; (d) Errado. Uma bridge é um dispositivo que conecta redes locais diferentes e pode operar em várias topologias. No entanto, sua função principal é conectar redes, não necessariamente em topologias de estrela (Letra B).

#VamosPraticar#

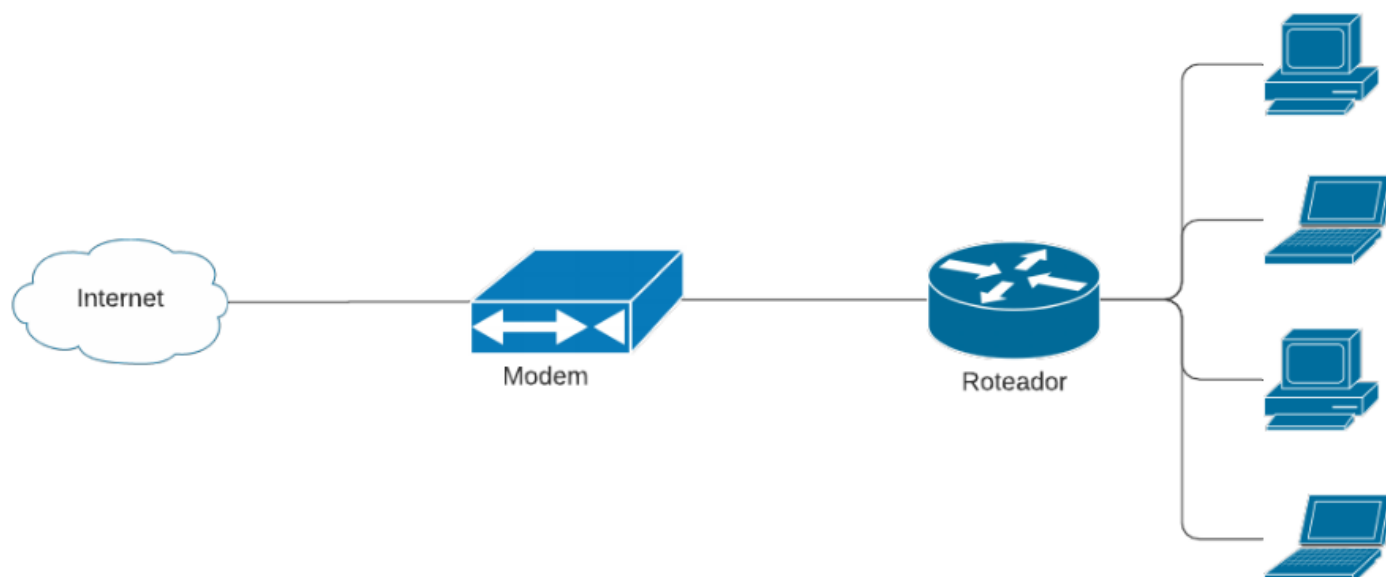
Router (Roteador)

INCIDÊNCIA EM PROVA: ALTA

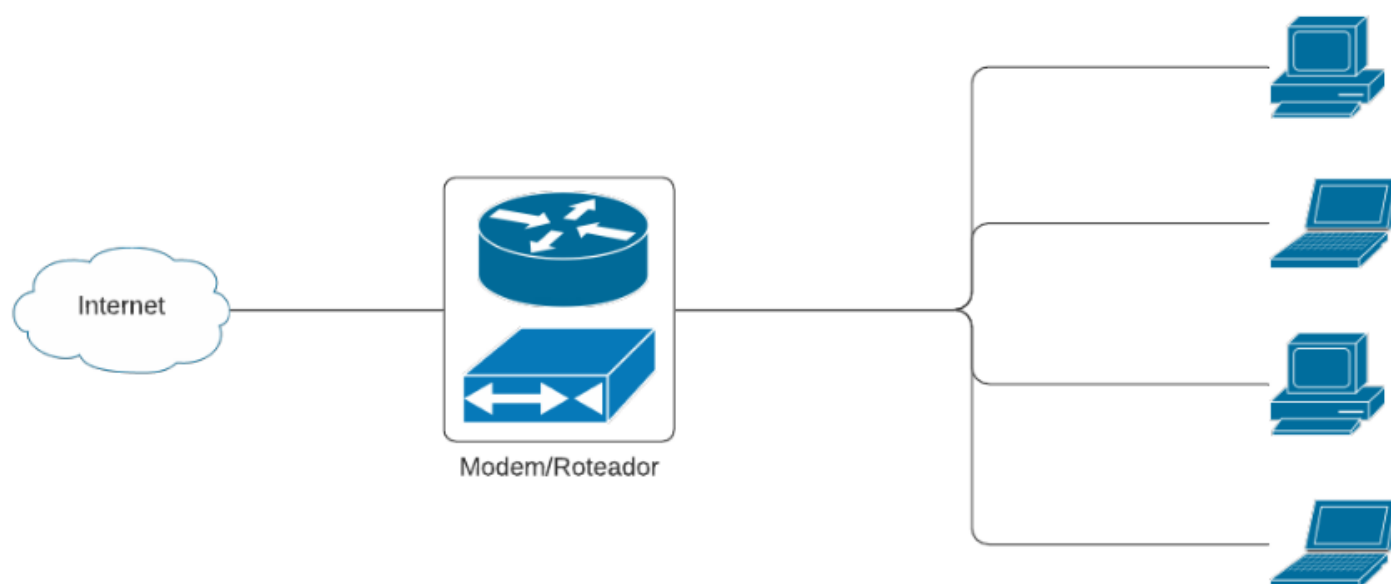


Os roteadores são equipamentos que permitem interligar redes diferentes e escolher a melhor rota para que uma informação chegue ao destino. Esse dispositivo encaminha ou direciona pacotes de dados entre redes de computadores, geralmente funcionando como uma ponte entre redes diferentes. Hoje em dia, são muito comuns em residências para permitir a conexão entre redes locais domésticas (Rede LAN) e a Internet (Rede WAN).

Quem é mais velho se lembrará que uma configuração muito comum em casas antigamente consistia em um modem, um roteador e até quatro dispositivos. **O modem era responsável por receber o sinal de internet (veremos em detalhes mais adiante) e o roteador era responsável por interligar os quatro computadores à internet.** Por que somente quatro dispositivos, professor? Porque era o número máximo de portas em um roteador comum.



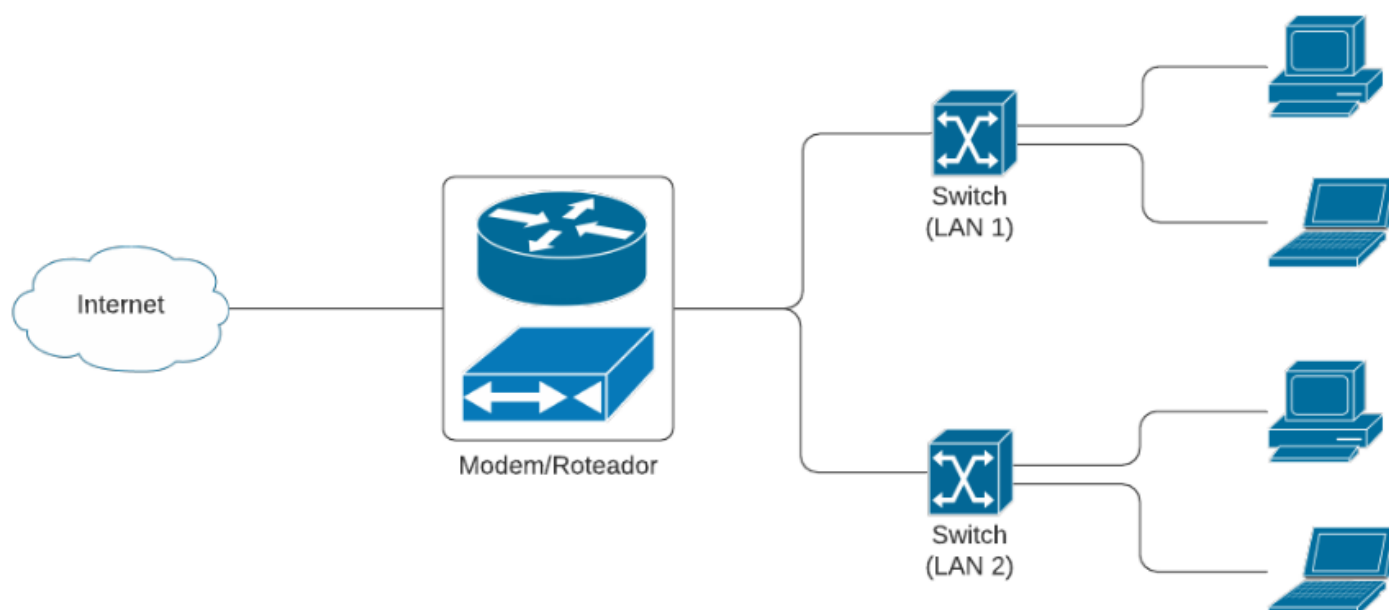
Atualmente, nós estamos na era dos combos, isto é, um único provedor fornece Internet, Telefone e TV a Cabo (Ex: NET/Claro, GVT/Vivo, etc). Nesse caso, um único aparelho condensa as funções de modem e roteador – você provavelmente tem esse aparelho na sua casa! Em geral, um cabo coaxial branco entra nesse dispositivo, que possui geralmente quatro portas. Em empresas, nós temos geralmente uma configuração um pouco diferente.



Primeiro, uma empresa pode ter uma centena de computadores, logo as quatro portas de um roteador não seriam suficientes. Além disso, ela pode ter redes locais diferentes dentro dela por motivos de segurança. *Como assim, Diego?* **Galera, é interessante separar dados sensíveis de dados não sensíveis em redes diferentes. Caso a rede de dados não sensíveis seja invadida, não afetará a rede de dados sensíveis, por exemplo.**

Dessa forma, uma terceira configuração pode ter um modem/roteador e dois switches, segmentando a rede local em duas, conforme apresenta a imagem à esquerda. Já na imagem à direita, temos a parte traseira de um roteador: observem que temos quatro portas em amarelo

e uma porta azul. As portas amarelas – Portas LAN – são dedicadas a conectar equipamentos da rede interna e a porta azul – Porta WAN – é utilizada para conectar uma rede externa (Internet).



Um roteador pode ser com fio ou sem fio (wireless). Atualmente, a maioria dos roteadores do mercado são sem fio – apesar de permitirem conexão cabeada também. Nós já sabemos que um roteador é capaz de interligar redes diferentes. **No entanto, um roteador wireless é um dispositivo mais flexível, podendo trabalhar em outros três modos diferentes: Hotspot, Access Point ou Repetidor de Sinal.** Vamos falar sobre cada um deles...

No modo Hotspot, o roteador tem o simples objetivo de oferecer acesso à internet. Como assim, Diego? Vamos imaginar que você enjoou de estudar informática em casa e resolveu levar seu notebook e estudar em uma cafeteria. Você chama o garçom, pede um espresso, uma água e... a senha do wi-fi! Vamos supor que a rede local da cafeteria é composta por cinco computadores, uma impressora e um banco de dados conectados em rede.

Ora... se o roteador wireless da cafeteria estiver configurado em modo hotspot, eu terei acesso simplesmente à internet, mas não terei acesso a notebooks de outros clientes ou aos computadores, impressora e banco de dados da cafeteria. **O hotspot é – apenas e tão somente – um local onde uma rede sem fio está disponível para ser utilizada.** Alguns estabelecimentos oferecem de forma gratuita (bares, restaurantes, etc) e outros são pagos (aeroportos e hotéis).



Atualmente, é possível configurar até o próprio celular como um hotspot. *Quem aí já compartilhou o 4G do celular com um amigo?* Se sim, você configurou seu celular como um hotspot! Agora eu gostaria que vocês fizessem um experimento social: na próxima vez que vocês forem a um bar, restaurante, academia, estádio, universidade, aeroporto, etc, olhem para o teto ou para as paredes! **Eu tenho certeza que vocês encontrarão vários dispositivos como esses da imagem ao lado: Hotspots.**

O segundo modo de configuração de um roteador wireless é como Access Point. **Nesse caso, a ideia é estender os recursos da rede local para a rede sem fio.** Quando um roteador wireless é configurado no modo Hotspot, a ideia era oferecer acesso à internet e, não, aos outros recursos de rede compartilhados. Já quando ele é configurado no modo Access Point, ele oferece – sim – acesso a todos os recursos da rede.

Apesar dessa diferença, é importante mencionar que um Hotspot pode ser considerado um Access Point de acesso público – algumas provas os consideram sinônimos. Por fim, esse roteador wireless pode também ser configurado como repetidor de sinais. *Sabe quando você se deslocar da sala um quarto distante ou de um andar para outro em uma casa e o sinal da wi-*

fi piora vertiginosamente? Pois é, o repetidor vai regenerar o sinal e propagá-lo por uma distância maior.

Apesar de existirem essas configurações do roteador wireless, é possível comprar um Hotspot, Access Point ou Repetidor de Sinal separadamente. No entanto, é importante salientar que todo roteador wireless é capaz de funcionar como um Hotspot, Access Point ou Repetidor de Sinal, porém o contrário nem sempre é verdadeiro. Por exemplo: nem todo Access Point é capaz de funcionar como um roteador. *Fechou?*



Qual é a diferença entre um Roteador e um Access Point?

Uma pergunta frequente no fórum de dúvidas é: qual é a diferença entre um Roteador e um Access Point? Em primeiro lugar, nós já vimos que um Roteador pode ser configurado para funcionar como um Access Point. Em segundo lugar, um Roteador tem o objetivo de interligar redes diferentes. Já um Access Point tem o objetivo de estender os recursos da rede local para a rede sem fio.

CARACTERÍSTICA	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo de rede que filtra, encaminha e controla pacotes de dados entre redes, determinando a melhor rota com base em endereços IP.
CAMADA OSI	Camada 3 (Rede).
VANTAGENS	Roteia tráfego entre redes, permitindo conectividade inter-redes; ajuda a dividir redes em sub-redes para melhor organização e segurança.
DESVANTAGENS	Pode ser mais complexo de configurar em comparação com switches/hubs; pode ser um ponto único de falha se não houver

redundância.

#VamosPraticar#

(IDECAN / IF-PB – 2019) A respeito dos diversos tipos de equipamentos de rede, assinale a alternativa que indica corretamente o nome do equipamento de rede capaz de realizar uma conexão entre diferentes redes de modo a permitir a troca de informações entre elas, mas que seja capaz também de controlar o fluxo da informação, possibilitando, por exemplo, a criação de rotas mais curtas e rápidas:

- a) Modem
- b) Repetidor
- c) Bridges
- d) Switch
- e) Roteador

Comentários: conexão entre diferentes redes (Ex: Internet e LAN) e controlar fluxo de informações pelas rotas são responsabilidades do roteador (Letra E).

(IBADE / Prefeitura de João Pessoa-PB – 2018) Um equipamento de rede que permite que computadores de uma rede possam se conectar a Internet é o:

- a) HDCCD.
 - b) pen drive.
 - c) roteador.
 - d) scanner.
 - e) VGA.
-

Comentários: o dispositivo responsável por permitir a conectividade entre dispositivos como computadores, smartphones, tablets, etc em uma Rede LAN com a internet é o Roteador (Letra C).

#VamosPraticar#

Modem

INCIDÊNCIA EM PROVA: média



Galera, imaginem que eu preciso enviar um e-mail para o Prof. Renato! **Para que essa mensagem saia do meu computador e chegue no computador dele, é necessário que ela seja transmitida por um meio de comunicação.** Pode ser através de fibras ópticas, ondas de rádio, entre outros – no entanto há uma alternativa interessante de infraestrutura que já existe na imensa maioria dos lugares. *Qual, professor?* A infraestrutura de linha telefônica!

Isso não é tão simples assim, porque os computadores possuem uma linguagem diferente da linguagem dos telefones. Quando eu envio um e-mail para o Prof. Renato, a mensagem é convertida em um conjunto de dígitos binários (Ex: 011010001000111010). Os telefones não conseguem entender essa linguagem porque eles utilizam sinais analógicos que, inclusive, não

são entendidos por computadores. É como se um falasse húngaro e o outro aramaico!

Como resolver esse problema? **Evidentemente nós precisamos de um tradutor!** E é aí que entra o papel do Modem (**Mod**ulador/**Dem**odulador). Esse dispositivo converterá os dígitos binários do meu computador em sinais analógicos que podem ser transmitidos em linhas telefônicas; e também converterá os sinais analógicos das linhas telefônicas em dígitos binários. *Ficou mais fácil de entender agora?* Então vamos ver a definição...



O Modem é um dispositivo eletrônico de entrada/saída de dados que modula um sinal digital em um sinal analógico a ser transmitida por meio de uma linha telefônica e que demodula o sinal analógico e o converte para o sinal digital original. **Hoje em dia, existem basicamente três tipos: Acesso Discado, Modem ADSL e Cable Modem.**

O Modem de Acesso Discado é inserido na placa-mãe do seu computador. Quem aí é mais velho sabe que antigamente a internet era bem lenta e muito cara! *Sabe como eu fazia para me conectar à internet?* Eu esperava passar de meia-noite (porque o minuto cobrado ficava bem mais barato), desconectava o cabo do telefone fixo e conectava esse mesmo cabo no modem de acesso discado na parte de trás do gabinete do computador. O telefone, é claro, parava de funcionar!

Depois disso, você abria um discador e tinha que fazer infinitas tentativas para conseguir se conectar! Quando você finalmente conseguia, você ficava todo feliz, mas demorava mais ou menos uns dois minutos para abrir qualquer página na internet e quando ela estava quase toda aberta... a conexão caía! É, criançada... a vida era um bocado mais difícil, mas era divertido! Deixa eu contar uma historinha que aconteceu comigo...

Naquela época, poucas pessoas tinham condição de possuir um celular. Se você quisesse falar com alguém, teria que ligar em um telefone fixo e torcer para que o destinatário estivesse no local. Minha irmã mais velha estava grávida de nove meses e eu – aos 13 anos – estava doido para que chegasse meia-noite, **assim eu poderia acessar à internet de graça e ler meus fóruns sobre o jogo que virou febre na época: Pokemon (não é Pokemon Go, eu sou raiz...).**



Como vocês sabem, ao se conectar utilizando um Modem Dial-Up, o telefone ficava ocupado. Você não conseguiria ligar para ninguém e, se alguém te ligasse, ouviria o sinal de ocupado. Ocorre que a bolsa da minha irmã estourou e nem ela nem o esposo possuíam carro, logo ela ligou para minha mãe buscá-la. *O que aconteceu?* Tu-tu-tu-tu-tu – sinal de ocupado porque eu estava vendo meus fóruns. *Tomei uma surra monumental: sim ou não?* Pois é! Ainda bem que ela conseguiu outro transporte e meu sobrinho está hoje com 20 anos! **Até que chegaram os Modems ADSL.**

Empresas de telefonia fixa ofereciam acesso em banda larga^[9] por meio de cabos ou wireless. Pessoal, era muito mais rápido (velocidade de download/upload) e não ocupavam o telefone, ou seja, você podia utilizar o telefone e a internet simultaneamente. Por fim, temos o Modem Cabeado (*Cable Modem*)! Eles não utilizam as linhas telefônicas – eles são conectados por meio de cabos coaxiais normalmente fornecido pela sua fornecedora de TV a Cabo. *Como é, professor?*

Você tem NET ou GVT? Pois é, elas te oferecem serviços diferentes! Um serviço interessante é o combo: TV, Internet e Telefone! Em vez de utilizar três meios para te fornecer cada um desses serviços, ela transmite todos esses dados via cabo coaxial. **Algumas vezes, esse**

modem virá com um roteador acoplado internamente; outras vezes, você terá que comprar um roteador e utilizar ambos para ter acesso à internet. *Entendido?* Então vamos seguir...

Uma dúvida que aparece de vez em quando no fórum trata de Gateway. Esse equipamento tem a função de interligar redes com arquiteturas e protocolos diferentes permitindo que essas duas redes distintas possam se comunicar, realizando a conversão entre os protocolos de cada uma das redes – qualquer equipamento que realize essa função genericamente é chamado de gateway. Ele geralmente trabalha em todas as camadas da Arquitetura TCP/IP (veremos em outra aula).

Modem	DESCRIÇÃO
DEFINIÇÃO	Dispositivo que modula e demodula sinais para permitir a comunicação digital através de meios analógicos, como linhas telefônicas.
CAMADA OSI	Camada 1 (Física) e 2 (Enlace).
VANTAGENS	Permitem a comunicação de dados através de redes analógicas; são amplamente utilizados para acesso discado à Internet; facilitam a conexão com redes de banda larga.
DESVANTAGENS	Velocidade de transmissão baixa comparada com tecnologias de banda larga; suscetíveis a ruídos em linhas telefônicas; largura de banda e capacidade de transmissão limitadas.

#VamosPraticar#

(QUADRIX / CRESS-SE – 2021) Caso o usuário possua somente um modem ADSL para acessar a Internet, não será possível compartilhar essa conexão na rede para outros usuários.

Comentários: é possível compartilhar uma conexão de Internet por meio de um modem ADSL com outros usuários em uma rede. Para fazer isso, normalmente é necessário utilizar um roteador. O roteador permite que vários dispositivos se conectem à Internet através do modem ADSL, compartilhando assim a conexão. Isso é um cenário comum em redes domésticas e de pequenos escritórios, onde diversos dispositivos, como computadores, laptops, smartphones e tablets, precisam acessar a Internet a partir de um único modem ADSL (Errado).

(IBADE / Prefeitura de Linhares-ES – 2020) Um dispositivo ao qual está conectada uma linha telefônica, permitindo a transmissão de dados através dela chama-se:

- a) Modem.
- b) Barramento.
- c) Switch.
- d) Hub.
- e) Transceiver.

Comentários: o dispositivo ao qual está conectada uma linha telefônica, permitindo a transmissão de dados através dela, é chamado de modem (Letra A).

(UFGD / UFGD – 2019 – Letra C) O modem é um dispositivo eletrônico que modula um sinal digital numa onda analógica, pronta a ser transmitida pela linha telefônica, e que demodula o sinal analógico e reconverte-o para o formato digital original.

Comentários: o modem realmente é um dispositivo utilizado para a conversão de sinais digitais em sinais analógicos para transmissão e vice-versa para recepção (Correto).

(CESPE / CET – 2011) O modem:

- a) é um tipo de memória semicondutora não volátil.
- b) é um tipo de interface paralela que permite a comunicação sem fio entre um computador e seus periféricos.
- c) é um roteador wireless para redes sem fio.
- d) tem função de garantir o fornecimento ininterrupto de energia elétrica ao computador.
- e) pode auxiliar na comunicação entre computadores através da rede telefônica.

Comentários: (a) Errado, modem não tem nenhuma relação com memória semicondutora; (b) Errado, modems são usados para comunicação de dados via linhas telefônicas ou redes semelhantes, mas não estão diretamente relacionados à comunicação sem fio entre

computadores e periféricos; (c) Errado, um modem e um roteador são dispositivos distintos. Enquanto o modem lida com a conversão de sinais para comunicação através da infraestrutura de rede, um roteador é responsável pela distribuição de conexões em redes locais, como redes sem fio (Wi-Fi); (d) Errado, isso descreve uma função de um no-break (UPS) ou um estabilizador de energia, não do modem; (e) Correto, O modem é projetado para auxiliar na comunicação entre computadores e outros dispositivos através da rede telefônica, convertendo os sinais digitais dos computadores em sinais analógicos que podem ser transmitidos pela linha telefônica e vice-versa (Letra E).

(FUNRIO / DEPEN – 2008) Quais as características a tecnologia de conexão à Internet denominada ADSL:

- a) Conexão permanente, custo fixo, linha telefônica liberada e velocidade maior do que as linhas tradicionais.
- b) Conexão permanente, custo variável, linha telefônica liberada e velocidade maior do que as linhas tradicionais.
- c) Conexão permanente, custo fixo, linha telefônica não liberada e velocidade maior do que as linhas tradicionais.
- d) Conexão não-permanente, custo variável, linha telefônica liberada e velocidade igual às linhas tradicionais.
- e) Conexão não-permanente, custo fixo, linha telefônica não liberada e velocidade igual às linhas tradicionais.

Comentários: *conexão permanente* – ADSL permite que você se mantenha sempre conectado, em contraste com as linhas tradicionais (Ex: Dial-up) em que – para acessar a internet – precisa se conectar; *custo fixo* – ADSL possui um custo fixo, visto que você não paga mais por conta do horário, etc, em contraste com linhas tradicionais em que você paga valores adicionais a depender do horário; *linha telefônica liberada* – ADSL permite que se utilize a internet e o telefone simultaneamente, em contraste com linhas tradicionais em que você ou utiliza a internet ou utiliza o telefone; *velocidade maior do que as linhas tradicionais* – ADSL possui a grande vantagem de permitir uma velocidade (muito) maior do que as linhas tradicionais (Letra A).

#VamosPraticar#

1.8 Redes de Computadores - Parte 1 - Padrões de Redes - Teoria



Para assistir ao vídeo correspondente, acesse o LDI.

Padrões de Redes

Seus lindos... existe lá nos Estados Unidos um instituto bastante famoso chamado IEEE (*Institute of Electrical and Electronics Engineers*)! Trata-se da maior organização profissional do mundo dedicada ao avanço da tecnologia em benefício da humanidade. **Esse tal de IEEE (lê-se “I3E”) mantém o Comitê 802, que é o comitê responsável por estabelecer padrões de redes de computadores.** Professor, o que seriam esses padrões de redes?

Padrões de Redes são uma especificação completamente testada que é útil e seguida por aqueles que trabalham com Internet – trata-se de uma regulamentação formal que deve ser seguida. **O Padrão IEEE 802 é um grupo de normas que visa padronizar redes locais e metropolitanas nas camadas física e de enlace do Modelo OSI.** Os padrões de rede descrevem vários aspectos das redes, incluindo:

Aspectos	Descrição
Meio de transmissão	Podem especificar se a rede é com ou sem fio. Também podem especificar a largura de banda e as características físicas do meio de transmissão.
Topologia	Podem definir a topologia da rede, como barramento, estrela, anel ou malha.
Protocolos	Podem definir protocolos de comunicação que os dispositivos de rede devem seguir para trocar dados, como protocolos de camada física e protocolos de camada de aplicação.
Segurança	Podem incluir diretrizes de segurança, como criptografia e autenticação, para proteger a rede contra ameaças.
Compatibilidade	Garantem que os dispositivos de diferentes fabricantes possam funcionar juntos na mesma rede, desde que sigam o mesmo padrão.
desempenho	Podem abordar questões de desempenho, como largura de banda, latência e qualidade de serviço.

Na tabela a seguir, é possível ver diversos padrões diferentes de redes de computadores que são comuns em provas de concurso:

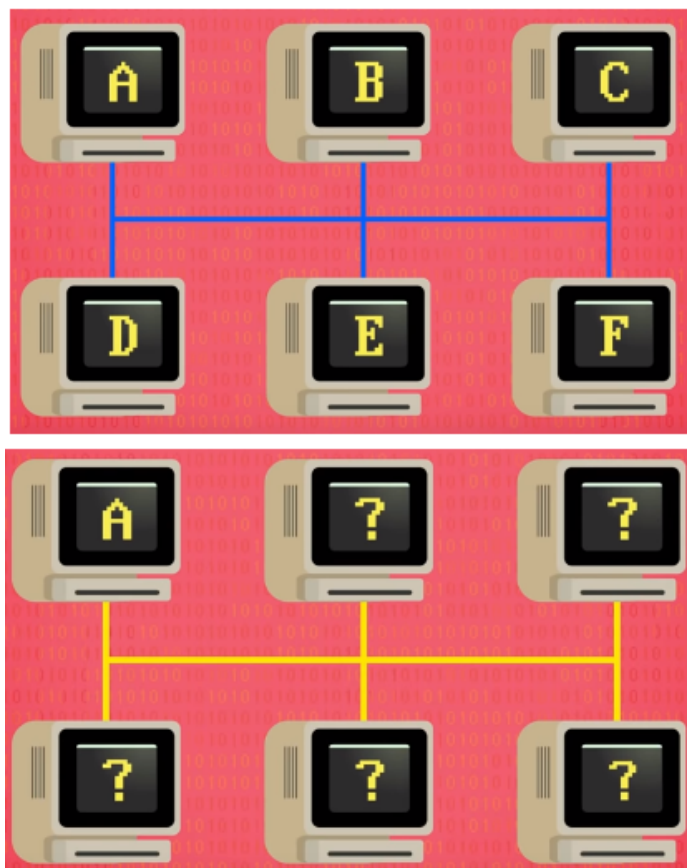
PADRÃO	NOME
IEEE 802.3	Ethernet (LAN) _[10]
IEEE 802.5	Token Ring (LAN)
IEEE 802.11	Wi-Fi (WLAN)
IEEE 802.15	Bluetooth (WPAN)
IEEE 802.16	WiMAX (WMAN)
IEEE 802.20	Mobile-Fi (WWAN)

Padrão Ethernet (IEEE 802.3)

INCIDÊNCIA EM PROVA: ALTA

Ethernet é um conjunto de tecnologias e padrões que permite que dois ou mais computadores se comuniquem utilizando meios cabeados em uma Rede de Área Local (LAN). Notem que eu afirmei que é um conjunto de tecnologias e padrões, portanto nós vamos estudá-los por partes. Em relação à topologia utilizada, pode ser em Barramento ou Estrela. Vamos falar inicialmente sobre Padrão Ethernet com topologia em barramento.

Nós já sabemos que essa topologia conecta todos os dispositivos a um único cabo comum (*backbone*). Quando um computador deseja transmitir dados a outro computador, ele traduz os dados em sinais elétricos e os envia pelo cabo. **Como o cabo é compartilhado, todo computador que estiver conectado à rede receberá os dados transmitidos, uma vez que a difusão ocorre em *broadcast*.** Lembra?



← Configurações

🏠 Dids&Deds2G

Servidores DNS IPv4: 8.8.8.8
8.8.4.4

Editar

Propriedades

Endereço IPv6: 2804:14c:6585:448a:1511:3a75:4af1:691f

Endereço IPv6 de link local: fe80::1511:3a75:4af1:691f%14

Servidores DNS IPv6: 2804:14d:1:0:181:213:132:2
2804:14d:1:0:181:213:132:3
2804:14d:1:0:181:213:132:2
2804:14d:1:0:181:213:132:3

Endereço IPv4: 192.168.0.10

Servidores DNS IPv4: 8.8.8.8
8.8.4.4

Fabricante: Intel

Descrição: Intel(R) Ethernet Connection (2) I219-V

Versão do driver: 12.18.8.4

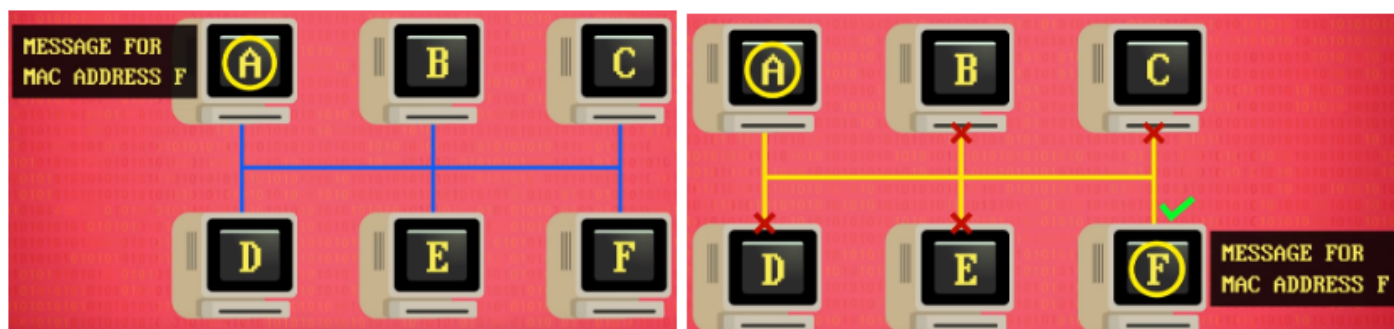
Endereço físico (MAC): 70-85-C2-81-1D-C4

Copiar

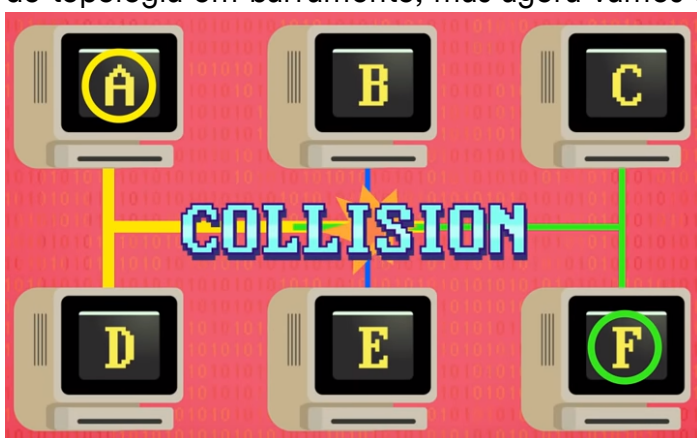
Na imagem acima, temos o *backbone* em azul porque nenhum sinal está sendo transmitido; e na imagem abaixo, temos o *backbone* em amarelo onde o sinal está sendo transmitido. **Notem que o backbone está todo amarelo porque – como a transmissão ocorre em broadcast – todas as máquinas o recebem.** Por outro lado, apesar de todos os computadores receberem os dados enviados, apenas o destinatário original poderá processá-los.

Professor, como os computadores vão saber se os dados recebidos de outro computador são direcionados a eles ou não? **Para resolver esse problema, a Ethernet requer que cada computador tenha um único endereço físico – também chamado de Endereço MAC (Media Access Control Address).** Esse endereço único é colocado em um prefixo junto com os dados a serem transmitidos (vejam na imagem anterior o Endereço MAC do meu computador).

Dessa forma, computadores na rede continuam recebendo os dados, mas só os processam quando eles verificam que é o endereço deles que está contido no prefixo. Vejam abaixo que o Computador A deseja enviar uma mensagem para o Computador F. Para tal, ele coloca o Endereço MAC do Computador F no prefixo da mensagem, que será processada por esse computador e ignoradas pelos outros. Toda placa de rede de um computador possui um Endereço MAC único!



O termo genérico para essa abordagem vista acima é **Carrier Sense Multiple Access (CSMA)**, também conhecido como **Acesso Múltiplo com Detecção de Portadora**. Em outras palavras, trata-se de um protocolo utilizado na Ethernet para monitorar o meio de transmissão e evitar colisões quando ocorrem múltiplos acessos. Nós já estudamos esse problema no tópico de topologia em barramento, mas agora vamos detalhar um pouco mais.



Infelizmente, utilizar um meio de transmissão compartilhado possui desvantagens. Quando o tráfego na rede está baixo, computadores podem simplesmente esperar que ninguém esteja utilizando o meio de transmissão para transmitir seus dados. No entanto, à medida que o tráfego aumenta, a probabilidade de que dois ou mais computadores tentem transmitir dados ao mesmo tempo também aumenta.

Quando isso ocorre, temos uma colisão!

A colisão deixa os dados ininteligíveis, como duas pessoas falando ao telefone ao mesmo tempo – ninguém se entende! Felizmente, computadores podem detectar essas colisões por meio de um protocolo chamado *Collision Detection*. Quando duas pessoas começam a falar ao mesmo tempo ao telefone, a solução mais óbvia para resolver esse problema é **parar a transmissão, esperar em silêncio e tentar novamente**. Ora... aqui é exatamente do mesmo jeito!

O problema é que o outro computador também vai tentar a mesma estratégia. Além disso, outros computadores da mesma rede podem perceber que o meio de transmissão está vazio e tentar enviar seus dados. *Vocês percebem que isso nos leva a mais e mais colisões?* Pois é, mas a Ethernet possui uma solução simples e efetiva para resolver esse problema. **Quando um computador detecta uma colisão, eles esperam um breve período de tempo antes de tentar novamente.**

Esse período poderia ser, por exemplo, um segundo! *Professor, se todos os computadores esperarem um segundo, isso não vai resultar no mesmo problema anterior?* Isso é verdade! Se todos esperarem um segundo para retransmitir, eles vão colidir novamente após um segundo.

Para resolver esse problema, um período aleatório – chamado de backoff – é adicionado: um computador espera 1,3 segundos; outro espera 1,5 segundos; e assim por diante.

Lembrem-se de que – para o mundo dos computadores – essa diferença de 0,2 segundos é uma eternidade. Logo, o primeiro computador verá que o meio de transmissão não está sendo utilizado e pode transmitir seus dados. 0,2 segundos depois, o segundo computador verá que o meio de transmissão não está sendo utilizado e poderá transmitir seus dados. *Professor, calma aí, isso ajuda bastante, mas e se tivermos muitos computadores não resolverá o problema!*

Para resolver esse problema, nós temos mais um truque! Sabemos que se um computador detecta uma colisão, ele esperará um segundo mais um tempo aleatório. Se mesmo assim houver outra colisão, pode ser que a rede esteja congestionada, logo ele não esperará mais um segundo, esperará dois segundos. Se mesmo assim houver colisão, esperará quatro segundos. **Se continuar havendo colisões, esperará oito segundos, e assim por diante até conseguir transmitir.**

Você – meu melhor aluno – vai continuar argumentando que isso não resolve o problema para muitos computadores. Imaginem uma universidade inteira com 1000 alunos acessando simultaneamente a rede local em um, e apenas um, cabo compartilhado. *Complicado, não é?* **A topologia em barramento possui várias limitações, tanto que atualmente está em completo desuso.** A coisa está ficando legal...

#VamosPraticar#

(QUADRIX / CRMV-MS – 2022) Uma das desvantagens das redes ethernet é que todas as estações possuem acesso à rede de maneira diferente, com relação ao tempo de acesso.

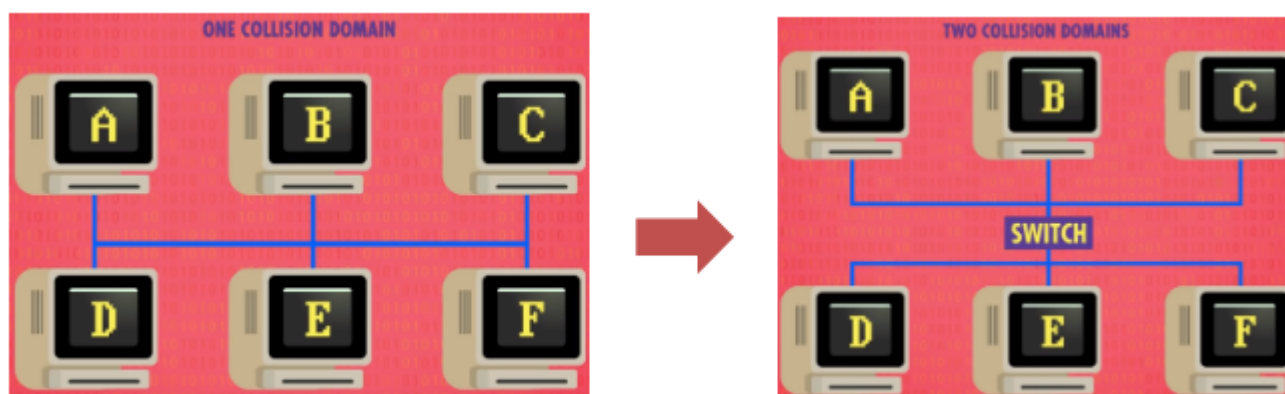
Comentários: em redes Ethernet, todas as estações acessam a rede de maneira semelhante – por meio do protocolo CSMA/CD. Várias estações compartilhem o mesmo meio de transmissão e quando uma estação deseja transmitir dados, verificam se o meio está ocupado (*Carrier Sense*) e, se estiver livre, a estação começa a transmitir. Se duas estações tentarem transmitir ao mesmo tempo e ocorrer uma colisão, ambas detectarão a colisão (*Collision Detection*) e interromperão suas transmissões – após uma pausa aleatória, ambas tentarão de novo (Errado).

#VamosPraticar#

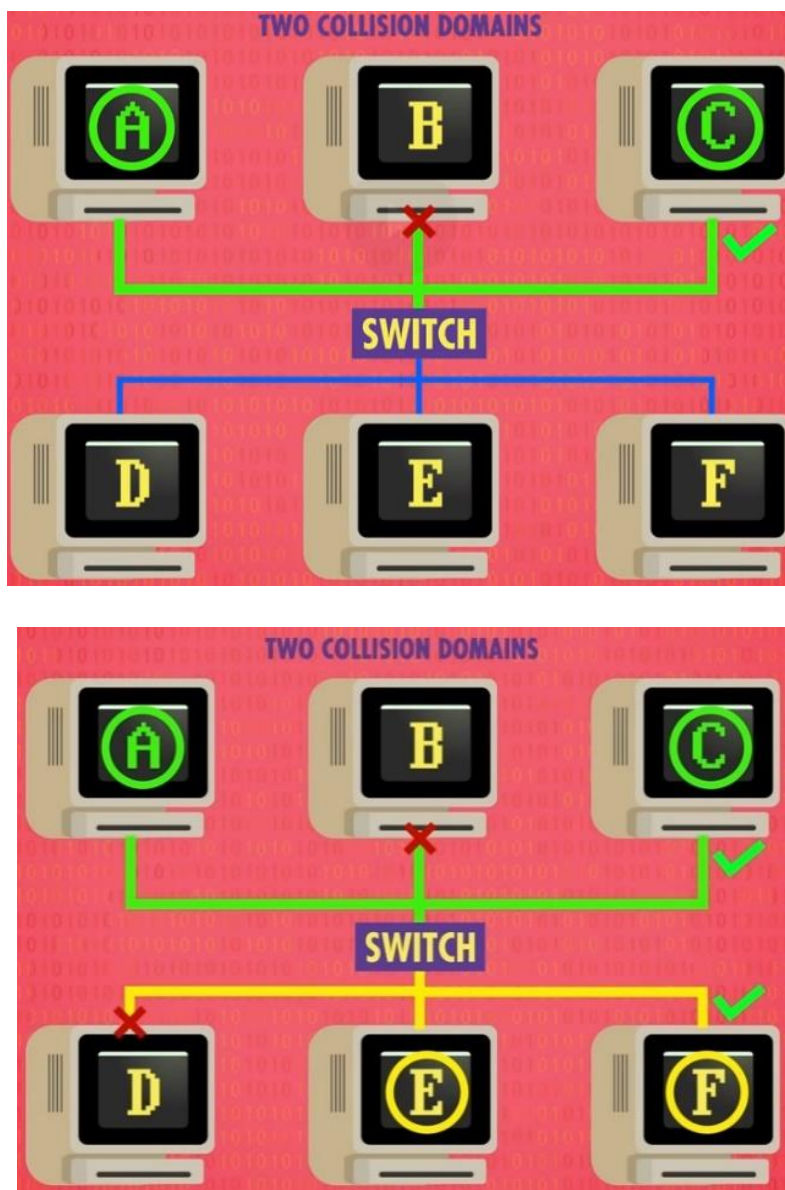
Para reduzir o número de colisões e melhorar a eficiência, nós precisamos diminuir a quantidade de dispositivos nos meios de transmissão compartilhados. Nesse momento, entra o conceito de Domínio de Colisão. O que é isso, Diego? Trata-se de uma área onde pacotes podem colidir uns contra os outros. A ideia aqui é segmentar a nossa rede em domínios de colisão menores, reduzindo – portanto – a probabilidade de colisões.

Pequena analogia para entender o que é um domínio de colisão: Imagine um corredor estreito em uma escola, em que os alunos estão indo para as aulas. Cada aluno representa um dispositivo de rede, como um computador. O corredor é a rede de cabos físicos ou meio compartilhado (por exemplo, um cabo Ethernet) que permite que os dispositivos se comuniquem.

Dessa forma, um domínio de colisão em uma rede Ethernet é como o corredor estreito em que os dispositivos precisam coordenar seu acesso para evitar colisões e permitir uma comunicação eficiente. Cada domínio de colisão representa uma área onde as colisões podem ocorrer, e as redes Ethernet foram projetadas para minimizar essas colisões e tornar a comunicação confiável.

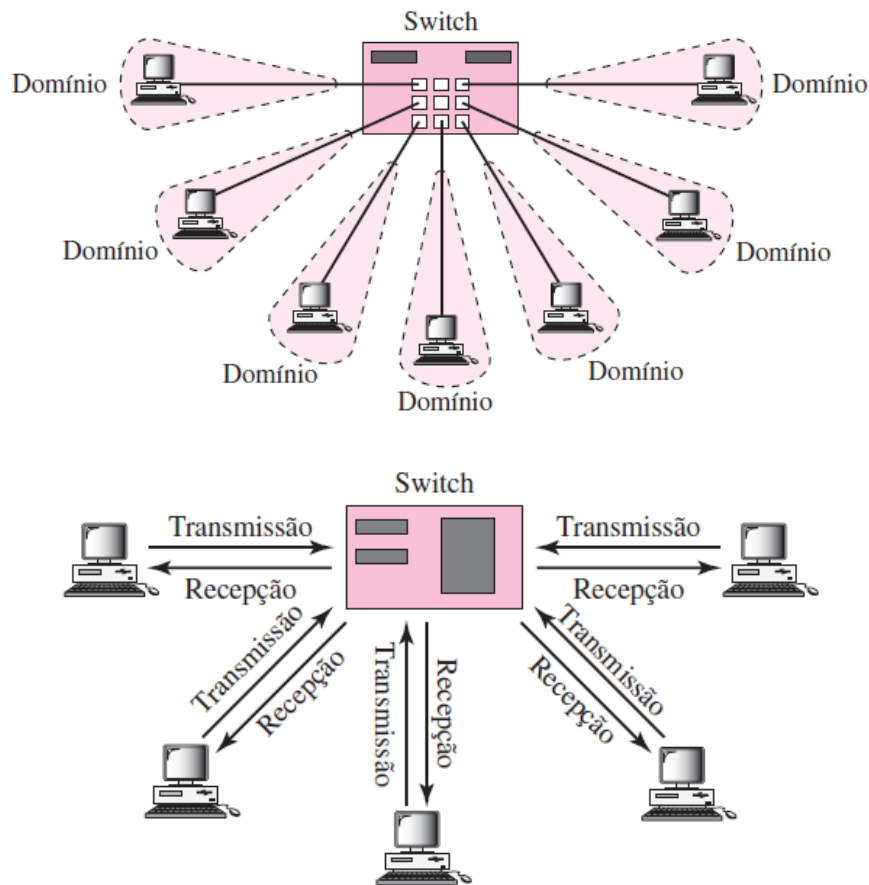


No exemplo anterior, nós tínhamos seis computadores conectados em um único meio de transmissão compartilhado, logo nós tínhamos um único domínio de colisão. Para reduzir a probabilidade de colisões, nós podemos segmentar a rede em dois domínios de colisão. Como, Diego? Nós podemos utilizar uma topologia em estrela com uso de um switch ^[11]. **Ele segmentará nossa rede em duas partes e ficará posicionado entre elas.**



Dessa forma, ele só passará dados para o outro domínio de colisão se a mensagem for destinada a algum computador presente nesse domínio de colisão. *Como ele faz isso, professor?* Ele guarda uma lista de Endereços MAC dos computadores de cada rede. **Assim, se o Computador A deseja transmitir dados para o Computador C, o switch não encaminhará os dados para o outro domínio de colisão – como mostra a imagem acima à esquerda.**

Notem que, se o Computador E quiser transmitir dados para o Computador F ao mesmo tempo que o Computador A transmite dados para o Computador C, a rede estará livre e as duas transmissões poderão ocorrer simultaneamente porque temos duas comunicações ocorrendo em dois domínios de colisão diferentes – como mostra a imagem acima à direita. **Percebam que os domínios de colisão criados reduziram as chances de colisões na rede.**



E digo mais: é possível criar um domínio de colisão para cada uma das portas de um switch (conforme apresenta à esquerda). Dessa forma, é possível eliminar toda e qualquer colisão!

Além disso, lembremos que o switch trabalha em full-duplex, ou seja, é capaz de enviar e receber dados simultaneamente, logo não há nenhuma chance de haver colisões! A probabilidade foi reduzida à zero e o nosso problema foi resolvido! :)

#VamosPraticar#

(CONSULPAM / ICTIM-RJ – 2023) Nas redes de computadores, é possível que ocorra uma colisão entre pacotes de dados quando duas ou mais estações pertencentes ao mesmo segmento de rede compartilhado transmitem quadros ao mesmo tempo. Assinale a alternativa que traz CORRETAMENTE um exemplo de domínio de colisão.

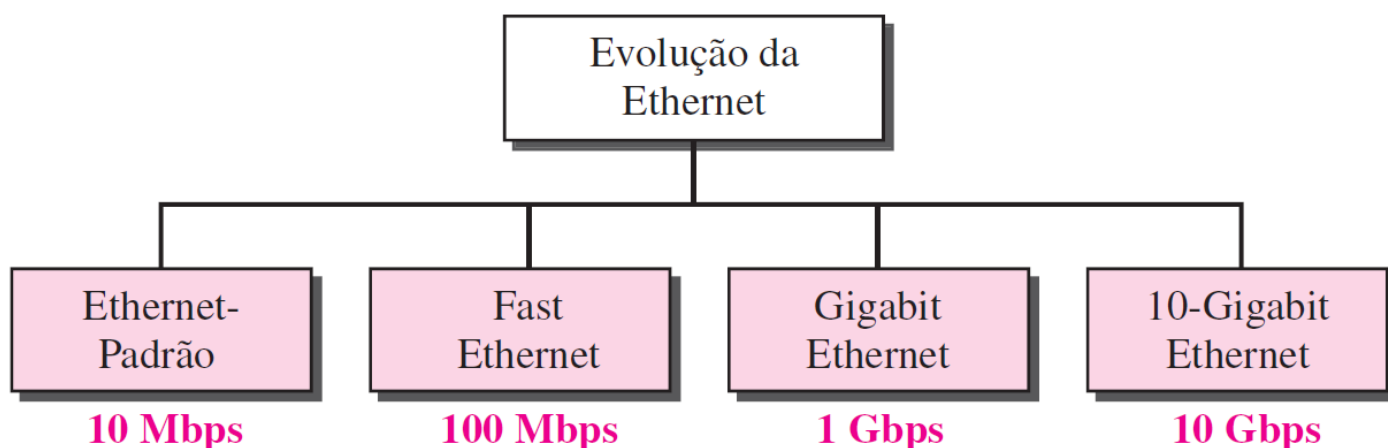
- a) Todos os dispositivos estão conectados a um hub ethernet.
- b) Todos os dispositivos estão conectados a um comutador ethernet.
- c) Todos os dispositivos estão conectados a um roteador wireless.
- d) Dois computadores, ambos conectados através de um cabo crossover.

Comentários: (a) Correto. Quando todos os dispositivos estão conectados a um hub Ethernet, eles compartilham o mesmo segmento de rede e fazem parte do mesmo domínio de colisão; (b) Errado. Nesse caso, cada porta do comutador (switch) cria seu próprio domínio de colisão, o que significa que as colisões são evitadas na medida do possível; (c) Errado. Os dispositivos estão conectados a um roteador wireless, que não compartilha o mesmo meio físico, logo não é um domínio de colisão; (d) Errado. Apenas dois computadores estão conectados através de um cabo crossover, o que significa que não há mais dispositivos no mesmo segmento de rede (Letra A).

#VamosPraticar#

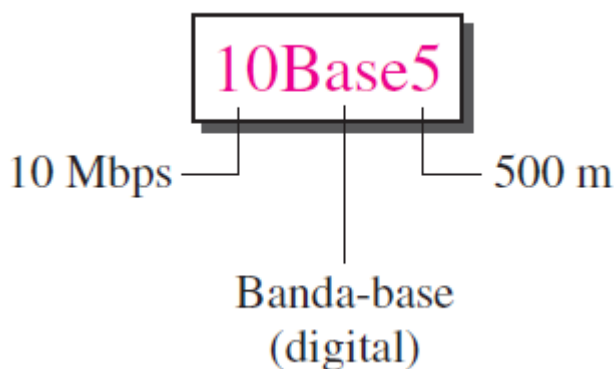
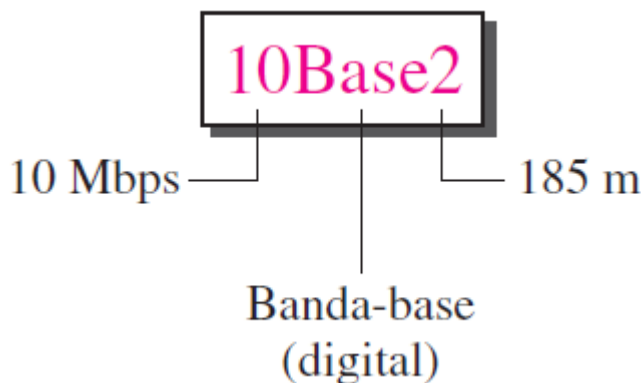
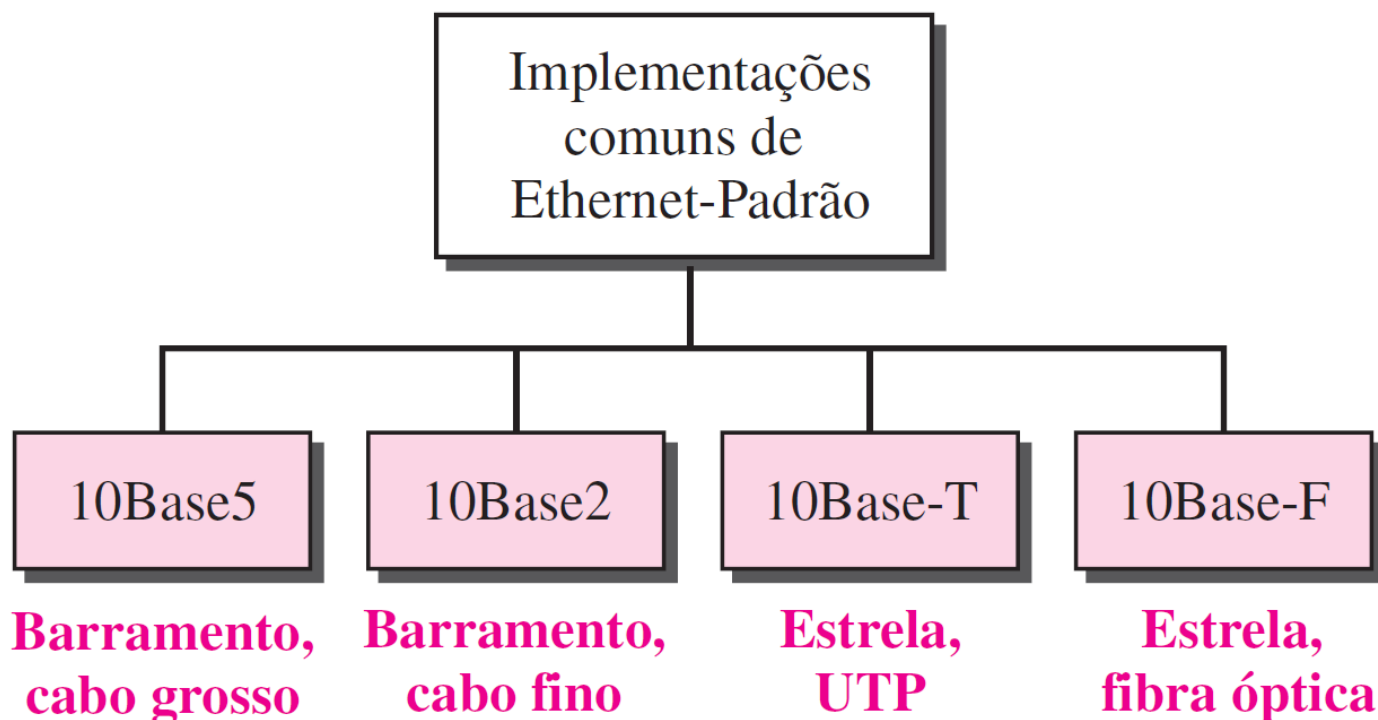
O que temos até agora sobre o Padrão Ethernet? **Sabemos que ele pode funcionar por meio da topologia em barramento.** Como pode haver colisões, entra em ação o CSMA/CD, que utiliza um algoritmo para evitar colisões. Ainda assim, sabemos que a topologia em barramento tem diversas limitações, inclusive em relação a colisões em um contexto de uma rede com muitos computadores. Podemos utilizar a topologia em estrela com um hub, mas retornaríamos ao mesmo problema.

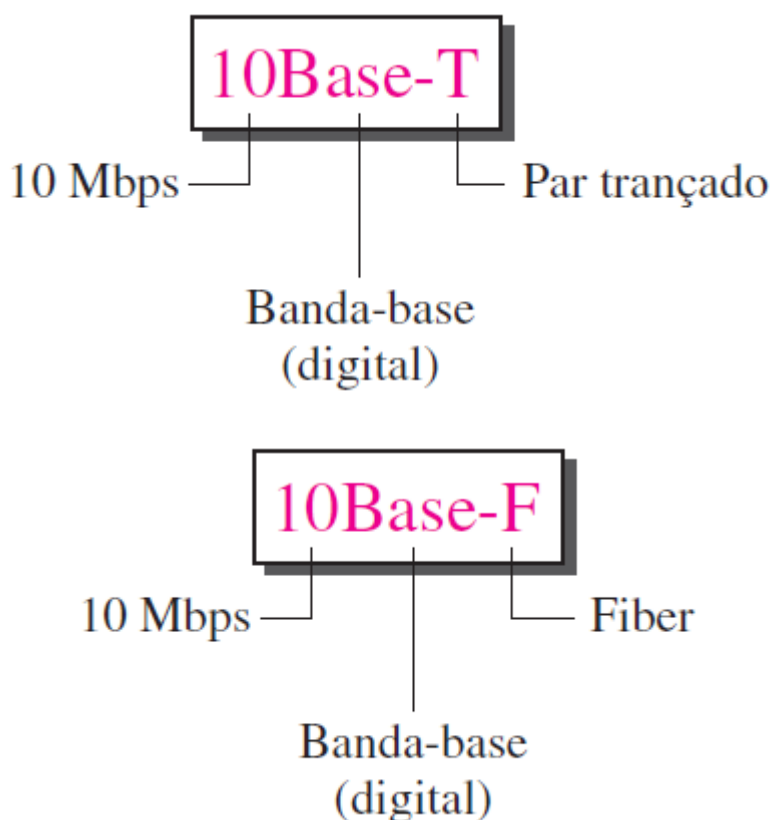
Para superar essa limitação, podemos utilizar a topologia em estrela com um switch. Por que? Porque ele funciona em full-duplex e segmenta a rede em domínios de colisão – eliminando chances de colisões e o seu consequente congestionamento da rede. Tudo isso que falamos diz respeito à Ethernet-Padrão, porém existem outras gerações: Ethernet-Padrão (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps) e 10 Gigabit Ethernet (10 Gbps). Estudaremos cada uma delas...



A Ethernet-Padrão possui quatro implementações comuns apresentadas na imagem seguinte. Vamos entender isso melhor? Note que temos um padrão: **NúmeroBaseNúmero** ou

NúmeroBase-Letra. Em laranja, temos a taxa de transmissão (Ex: **10Base2** trabalha com 10Mbps); em azul, temos a distância máxima (Ex: **10Base5** percorre no máximo 500 metros); em verde, temos o tipo de enlace (Ex: **10Base5** é cabo coaxial, **10Base-T** é par trançado e **10Base-F** é fibra óptica).





Esses se referem à Ethernet-Padrão! *E quanto às outras evoluções?* **Bem, temos a Fast Ethernet, que é compatível com as versões anteriores da Ethernet-Padrão, mas é capaz de transmitir dados dez vezes mais rápido, a uma velocidade de 100 Mbps.** Ainda havia necessidade de uma taxa de dados mais alta, logo surgiu o projeto do protocolo Gigabit Ethernet (1.000 Mbps ou 1Gbps). Por fim, surgiu o 10 Gigabit (10 Gbps).

EVOLUÇÃO DOS PADRÕES ETHERNET	
PADRÃO (CABO DE PAR TRANÇADO ou fibra óptica)	PADRÃO – TAXA máxima DE TRANSMISSÃO
Ethernet	10BASE-T / 10 Mbps
Fast Ethernet	100BASE-T / 100 Mbps
Gigabit Ethernet	1000BASE-T / 1000 Mbps
10G Ethernet	10GBASE-T / 10000 Mbps



Sabendo que Mega (M) = Milhão, Giga (G) = Bilhão e que 1G = 1000M, fica mais fácil lembrar que a Gigabit Ethernet tem a velocidade de 1000Mbps e que a 10G Ethernet tem a velocidade de 10.000Mbps. Além disso, uma largura de 100Gbps - por exemplo - permite transmitir até 100 Bilhões de bits por segundo (100.000.000.000 bits/segundo).

Vantagens do padrão ethernet	Desvantagens do padrão ethernet
Trata-se de uma das tecnologias de rede mais amplamente adotadas em todo o mundo.	Em redes Ethernet compartilhadas, as colisões de dados podem ocorrer, diminuindo o desempenho.
É relativamente fácil configurar e implantar, tornando-as acessíveis a muitas organizações.	Pode ser desafiador de escalar para redes maiores ou mais complexas.
Equipamentos e infraestruturas são geralmente mais acessíveis do que algumas alternativas.	Podem requerer cabeamento mais complexo e dispendioso.
Oferece boas taxas de transferência de dados e largura de banda adequada para muitos casos de uso.	Em redes Ethernet não criptografadas, os dados podem ser mais vulneráveis à interceptação.
A maioria dos dispositivos é compatível com Ethernet, facilitando a conectividade.	Em redes congestionadas, o desempenho do Ethernet pode diminuir.
Tende a ter latência baixa, o que é importante para aplicativos sensíveis à latência.	Não é adequada para redes sem fio, o que pode ser um problema em ambientes móveis.

#VamosPraticar#

(QUADRIX / CRMV-MS – 2022) Em função de o desenho das redes ethernet ser muito complexo, esse tipo de rede não permite manutenção após sua implementação.

Comentários: o desenho das redes Ethernet pode ser complexo, dependendo do tamanho e da topologia da rede, mas isso não significa que não permita manutenção após a implementação. Na realidade, as redes Ethernet são altamente mantidas e administradas, e as equipes de TI

frequentemente realizam tarefas de manutenção, como monitoramento, solução de problemas, atualizações e expansões, para garantir que a rede funcione de maneira eficiente e confiável. A complexidade pode exigir conhecimento e planejamento adequados, mas a manutenção é uma parte essencial da gestão de qualquer rede Ethernet (Errado).

#VamosPraticar#

Padrão Token Ring (IEEE 802.5)

INCIDÊNCIA EM PROVA: média

O Padrão Token Ring é outro padrão cabeado e foi, até o início da década de 90, o principal concorrente do Padrão Ethernet, quando possuía taxa de transmissão de dados de 4 Mbps, comunicação unidirecional (chamada *simplex*), arquitetura ponto-a-ponto e topologia lógica em anel. Por falar nisso, quando falamos em Topologia em Estrela, havia um risco de colisão – no Padrão Token Ring esse risco não existe porque utiliza Topologia em Anel.

Por que esse padrão se chama Token Ring? Isso ocorre basicamente porque cada estação de trabalho dessa rede de computadores se conecta com a adjacente até fechar um circuito fechado chamado Anel (*Ring*). Para que uma estação de trabalho possa transmitir dados para outra estação de trabalho, ela precisa possuir uma espécie de envelope chamado *token*. Vamos entender isso melhor...

Uma analogia que pode ser usada para explicar a comunicação no Token Ring é a de uma corrida de revezamento. Em uma corrida de revezamento, cada equipe tem um bastão que deve ser passado de um corredor para outro até que todos os corredores da equipe tenham completado uma volta na pista. Nós podemos dizer que um token é basicamente uma espécie de autorização ou envelope que dá ao dispositivo o direito de transmitir dados.

O token circula pela rede, de dispositivo em dispositivo, até que um dispositivo o pegue. Quando um dispositivo pega o token, ele pode transmitir os dados que deseja enviar. Assim como em uma corrida de revezamento, apenas um dispositivo na rede pode transmitir dados por vez. O token garante que os dispositivos não transmitam dados ao mesmo tempo, o que evitaria colisões de dados. Então seria mais ou menos assim...

O token é o bastão; o dispositivo que tem o token é o corredor que está com o bastão; os dados que o dispositivo está transmitindo são a mensagem que o corredor está carregando; e os outros dispositivos na rede são os espectadores da corrida. **A analogia da corrida de revezamento é uma maneira simples e fácil de entender o conceito de comunicação no Token Ring.** Vamos ver agora as principais vantagens e desvantagens desse padrão:

Vantagens do padrão token ring	Desvantagens do padrão token ring
O Token Ring é altamente confiável devido à sua estrutura em anel, que evita colisões de dados.	A implementação inicial do Token Ring pode ser mais cara devido ao hardware específico.
A topologia do anel elimina colisões de dados, o que leva a uma transmissão de alta qualidade.	Requer configuração complexa e habilidades técnicas para instalação e manutenção.
O tempo de latência é baixo, pois os dispositivos podem transmitir quando possuem o token.	Menos flexível do que outras topologias, tornando difícil adicionar ou mover dispositivos.
Permite a priorização de tráfego, garantindo que dados críticos sejam transmitidos primeiro.	A taxa de transmissão é geralmente mais baixa em comparação com tecnologias mais recentes.
Pode ser escalado facilmente, adicionando ou removendo dispositivos do anel.	O Token Ring é um padrão em declínio, com pouca inovação e suporte em comparação com Ethernet.

Por fim, vejamos agora uma pequena comparação entre os padrões **Ethernet** e **Token Ring** na tabela seguinte:

Característica	Padrão Token ring	Padrão Ethernet
topologia	Usa uma topologia em anel, onde os dispositivos são conectados em círculo e os dados são transmitidos em sequência – um dispositivo após o outro.	Usa uma topologia em estrela ou em barramento. Os dispositivos são conectados a um hub ou switch central.

Desempenho	Oferece um desempenho consistente devido à ausência de colisões de dados. A largura de banda é dividida igualmente entre os dispositivos no anel.	Pode ter colisões de dados, especialmente em redes ocupadas. A largura de banda é compartilhada entre todos os dispositivos na rede.
Custo	Geralmente é mais caro devido ao hardware específico necessário, como conectores de cabo MAU (<i>Media Access Unit</i>).	Geralmente é mais econômico, pois o hardware é amplamente disponível e menos caro.
implementação	Requer configuração mais complexa, como a definição de endereços de estação e prioridades de token.	É mais fácil de implementar, com menos requisitos de configuração.
Escalabilidade	Pode ser menos flexível para adicionar ou remover dispositivos sem interromper a rede.	É escalável e permite adicionar dispositivos com facilidade, especialmente em redes comutadas.
popularidade	Foi popular nas décadas de 1980 e 1990, mas agora é menos comum, pois a Ethernet se tornou dominante.	É a tecnologia de rede mais amplamente usada e suportada, com constante evolução.

Token Ring oferece confiabilidade e baixa latência devido à falta de colisões, mas tende a ser mais caro e menos flexível em termos de escalabilidade. A Ethernet é mais acessível, fácil de implementar e altamente escalável, embora possa ter colisões em redes congestionadas. A escolha entre as duas depende das necessidades específicas da rede e das limitações orçamentárias. *Entendido?*

Padrão Wi-Fi (IEEE 802.11)

INCIDÊNCIA EM PROVA: ALTA

A comunicação móvel está entre as tendências mais significativas, e os usuários esperam estar conectados à internet de forma contínua. A maioria dos hotéis oferece conexão online aos seus hóspedes, e as companhias aéreas agora disponibilizam serviços de internet em muitos de seus aviões. **A demanda por comunicação móvel tem despertado interesse pelas tecnologias wireless, e muitos padrões wireless foram criados.**

O Padrão Wi-Fi – diferentemente dos padrões anteriores – não é cabeado. Logo, um usuário pode ficar conectado mesmo deslocando-se num perímetro geográfico mais ou menos vasto – redes sem fio fornecem mobilidade aos usuários. **O Padrão Wi-Fi se baseia em uma conexão que utiliza infravermelho ou radiodifusão e define uma série de padrões de transmissão e codificação para comunicações sem fio.**

Sim, o controle remoto da sua televisão é um dispositivo wireless porque é capaz de trabalhar com infravermelho. *Qual é o problema dessa tecnologia?* Se houver algum obstáculo entre o controle e o receptor da televisão, a luz não atravessa e a comunicação não acontece. **Em outras palavras, é necessário ter uma linha de visada, isto é, uma linha sem obstáculos entre o emissor e o receptor.** Além disso, essa tecnologia permite apenas uma comunicação de curto alcance.

Foi, então, que surgiu a tecnologia de radiodifusão. Para tal, é necessário ter antenas e uma frequência comum de onda eletromagnética. *Qual é a grande vantagem dessa tecnologia?* Se houver uma parede entre as antenas, a onda consegue atravessá-la. Claro, pessoal... se for uma parede de um metro de espessura, provavelmente ela não conseguirá atravessar. E mesmo para paredes normais, haverá alguma perda, mas a comunicação funcionará normalmente.

Logo, podemos afirmar que a tecnologia de radiodifusão não trabalha com linha de visada, porque é capaz de atravessar obstáculos. Em contraste com o infravermelho, essa tecnologia tem como grande vantagem a ampla mobilidade. Um dispositivo cabeado tem baixíssima mobilidade, assim como o infravermelho (por conta da linha de visada). Por outro lado, um dispositivo com tecnologia de radiodifusão permite o deslocamento sem perda considerável de sinal.

Além disso, as redes wireless – em regra – possuem taxas de transmissão bem mais baixas. Vocês já devem ter notado que um download no computador ocorre bem mais rápido que um download em seu celular. *E as desvantagens, professor?* **Bem, toda tecnologia wireless é mais vulnerável a interceptações que redes cabeadas.** *Como, Diego?* Para interceptar dados em uma rede cabeada, é necessário ter acesso direto ao cabeamento (Ex: invadindo a casa de alguém).

Já para interceptar dados em uma rede wireless, é possível fazer a interceptação bastando estar próximo. Aliás, por essa razão, todo cuidado é pouco com a rede wireless da sua casa...

Risco	Descrição
Acesso não autorizado	Pessoas não autorizadas podem tentar se conectar à rede.
Interferência de sinal	Objetos físicos ou outras redes podem afetar a qualidade do sinal.
Ataques de força bruta	Tentativas de adivinhar senhas por meio de força bruta.
Monitoramento de tráfego	Espionagem do tráfego de rede para coletar informações.
Ponto de acesso falso	Atacantes podem criar redes falsas para enganar os usuários.
Vulnerabilidades de segurança	Falhas de segurança podem ser exploradas por invasores.
Ataques de negação de serviço	Sobrecarregar a rede para torná-la inacessível.
Uso excessivo de largura de banda	Usuários podem consumir toda a largura de banda disponível.
Compartilhamento inadequado	Compartilhamento de senhas com pessoas não confiáveis.
Configurações inadequadas	Configurações de segurança fracas ou inadequadas.

#VamosPraticar#

(QUADRIX / CRECI22 – 2023) O uso de redes Wi-Fi públicas não deve ser evitado, pois essas redes são totalmente seguras.

Comentários: é importante ter precauções ao usar redes Wi-Fi públicas, como evitar a transmissão de informações sensíveis e considerar o uso de uma VPN (Rede Virtual Privada) para criptografar sua conexão e proteger sua privacidade. Não é aconselhável considerar redes Wi-Fi públicas como totalmente seguras (Errado).

#VamosPraticar#



Percebam que Wireless é diferente de Wi-Fi. Wireless é qualquer tecnologia sem fio. **Wi-Fi (Wireless-Fidelity)** é uma marca registrada baseada no Padrão Wireless IEEE 802.11 que permite a comunicação entre computadores em uma rede sem fio (vejam que o logo possui um TM – TradeMark). Todo Wi-Fi é wireless, mas nem todo wireless é Wi-Fi.

Para resolver alguns destes riscos e proteger a integridade e a privacidade dos dados transmitidos, foram desenvolvidos mecanismos/protocolos de segurança, tais como:

Mecanismos	Descrição
Wep Wired equivalent privacy	O WEP foi um dos primeiros protocolos de segurança usados em redes Wi-Fi. No entanto, ele é considerado inseguro atualmente. Ele usa uma chave de criptografia compartilhada entre o roteador e os dispositivos para criptografar os dados que são transmitidos, mas tem vulnerabilidades que tornam relativamente fácil para um atacante comprometer a segurança da rede e acessar os dados. Devido a essas fraquezas, ele não é mais recomendado para uso.
Wpa Wi-fi protected access	O WPA foi desenvolvido para substituir o WEP e corrigir suas vulnerabilidades. Ele introduziu melhorias significativas na criptografia e na autenticação, tornando a rede mais segura. No entanto, ao longo do tempo, ele também mostrou algumas vulnerabilidades. Ele usa uma chave de segurança e um método de autenticação mais forte do que o WEP.
Wpa2 Wi-fi protected access 2	O WPA2 é uma evolução do WPA e é atualmente um dos protocolos de segurança mais seguros para redes Wi-Fi. Ele utiliza criptografia forte e o padrão IEEE 802.11i para proporcionar uma camada sólida de segurança. O WPA2 oferece autenticação forte e protege os dados transmitidos na rede Wi-Fi de maneira eficaz. É altamente recomendado configurar sua rede Wi-Fi com WPA2 para garantir a segurança.

Wpa3**Wi-fi
protected
access 3**

O WPA3 é uma versão mais recente que oferece ainda mais melhorias de segurança, incluindo criptografia mais forte e proteção contra-ataques de força bruta. Dessa forma, ao configurar uma rede Wi-Fi, é aconselhável usar WPA2 ou WPA3, se disponível, para garantir a proteção adequada.

#VamosPraticar#

(OBJETIVA / Prefeitura de Pedras Altas – 2022) Wi-Fi (Wireless Fidelity) é um tipo de rede local que utiliza sinais de rádio para comunicação. Redes Wi-Fi se tornaram populares; contudo, embora bastante convenientes, há alguns riscos, e, para resolver alguns desses riscos, foram desenvolvidos mecanismos de segurança. Sobre esses mecanismos de segurança, assinalar a alternativa que preenche as lacunas abaixo CORRETAMENTE:

O _____ foi o primeiro mecanismo de segurança a ser lançado, é considerado frágil e, por isso, seu uso deve ser evitado. O _____ é o mecanismo mais recomendado.

- a) WPA-2 | WPA
- b) WPA | WEP
- c) WEP | WPA-2
- d) WPA | WPA-2

Comentários: WEP foi o primeiro mecanismo de segurança a ser lançado, é considerado frágil e, por isso, seu uso deve ser evitado. O WPA-2 é o mecanismo mais recomendado (Letra C).

#VamosPraticar#

É importante também notar que redes wireless podem trabalhar em dois modos de operação: **Ad-hoc** ou **Infraestrutura**. A tabela apresentada a seguir oferece uma visão geral das diferenças entre redes wireless ad-hoc e redes wireless de infraestrutura. A escolha entre esses dois tipos de redes depende das necessidades específicas de um cenário de implementação, com base na topologia, escalabilidade e requisitos de segurança.

característica	Modo de operação Ad-hoc	Modo de operação infraestrutura
descrição	Comunicação direta entre equipamentos e válida somente naquele momento, conexão temporária, apresentando alcance reduzido (Ex: 5m).	Comunicação que faz uso de equipamento para centralizar fluxo da informação na WLAN (Ex: Access Point ou Hotspot) e permite um alcance maior (Ex: 500m).
Topologia de rede	Tipo de topologia de malha, onde cada dispositivo se conecta diretamente a outros dispositivos na rede.	Os dispositivos se conectam a um ponto de acesso central, como um roteador, que age como intermediário para encaminhar o tráfego.
Configuração de rede	Configurada sem a necessidade de um ponto de acesso central. Os dispositivos podem se comunicar diretamente uns com os outros.	Requer um ponto de acesso central (como um roteador) para gerenciar e encaminhar o tráfego na rede.
Flexibilidade	Mais flexível e útil em cenários onde não há acesso a uma infraestrutura de rede. Pode ser configurada rapidamente para conexões ponto a ponto.	Menos flexível em termos de implantação, pois depende de um ponto de acesso central. Ideal para redes com vários dispositivos em um único local.
Escalabilidade	Menos escalável para grandes redes devido à complexidade de gerenciar muitas conexões ponto a ponto.	Mais escalável para redes maiores, pois o ponto de acesso central gerencia eficientemente as conexões.
Segurança	Geralmente menos segura, pois não existe um ponto de controle central. As comunicações podem ser vulneráveis a ataques.	Mais segura, pois o ponto de acesso central pode implementar medidas de segurança, como criptografia e autenticação, em nome de todos os dispositivos.

Exemplos de utilização	Redes temporárias de curto prazo, comunicação direta entre dispositivos móveis (por exemplo, compartilhamento de arquivos entre smartphones).	Redes domésticas, redes empresariais, hotspots públicos e ambientes onde múltiplos dispositivos precisam se conectar a uma rede comum.
------------------------	---	--

#VamosPraticar#

(FUNDATEC / PROCERGS – 2023) O padrão 802.11 é o principal padrão de LAN sem fio chamada de Wireless Fidelity (Wi-fi). Atualmente, as redes Wi-fi tornaram-se bastante usuais pela mobilidade que proporcionam e pela facilidade de instalação e de uso em diferentes tipos de ambientes. Em relação à rede Wi-fi, analise assertivas abaixo:

- I. As redes Wi-fi são compostas de clientes, como notebooks e telefones móveis, e infraestrutura, chamada pontos de acesso ou Access Points (APs), que são instalados nos prédios.
- II. Este tipo de rede caracteriza-se por dois modos básicos de operação: o modo Infraestrutura (que faz uso de um concentrador de acesso ou roteador wireless) e o modo ponto a ponto (chamado ad-hoc, que permite criar redes pequenas, com as máquinas se comunicando entre si, sem o uso de um concentrador de acesso).
- III. Em redes Wi-Fi públicas, que não utilizam mecanismos de criptografia, os dados podem ser indevidamente coletados por atacantes.

Quais estão corretas?

- a) Apenas II.
- b) Apenas III.
- c) Apenas I e II.
- d) Apenas II e III.
- e) I, II e III.

Comentários: (I) Correto. Redes Wi-Fi são compostas por clientes (como notebooks, smartphones, tablets) e infraestrutura, que inclui os pontos de acesso ou Access Points, que são dispositivos instalados em prédios ou locais que fornecem a conectividade Wi-Fi; (II) Correto. Redes Wi-Fi possuem dois modos básicos de operação: o modo Infraestrutura é o mais comum, onde os dispositivos se conectam a um concentrador de acesso (como um roteador Wi-Fi) e o modo ponto a ponto (ad-hoc) permite que as máquinas se comuniquem diretamente entre si, sem a necessidade de um concentrador de acesso. Esse modo é útil para criar redes pequenas e temporárias; (III) Correto. Em redes Wi-Fi públicas que não utilizam mecanismos de criptografia, os dados transmitidos podem ser capturados por atacantes. Isso ocorre porque, sem criptografia, os dados são transmitidos em formato aberto, tornando-os vulneráveis à interceptação. É importante ter cuidado ao usar redes Wi-Fi públicas não seguras, especialmente ao lidar com informações sensíveis (Letra E).

#VamosPraticar#

Galera, alguém aí tem dispositivos da Apple? Se sim, vocês devem saber que existe uma funcionalidade chamada AirDrop, que permite a transferência de arquivos entre dispositivos Apple. Ao escolher o arquivo, o seu dispositivo identificará todos os outros dispositivos Apple próximos e uma conexão temporária será estabelecida. **Toda comunicação será descentralizada, direta entre os dispositivos, sem passar por um nó intermediário – logo, ela será ad-hoc.** [12]

EVOLUÇÃO DO PADRÃO wi-fi (802.11) [13]		
PADRÃO	FREQUÊNCIA	TAXA máxima DE TRANSMISSÃO
IEEE 802.11b	2.4 Ghz	11 Mbps
IEEE 802.11a	5.0 Ghz	54 Mbps
IEEE 802.11g	2.4 Ghz	54 Mbps
IEEE 802.11n	2.4 ou 5.0 Ghz	150, 300 até 600 Mbps
IEEE 802.11ac	5.0 Ghz	500 Mbps, 1 Gbps ou +
IEEE 802.11AX (wifi 6)	2.4 ou 5.0 Ghz	3.5Gbps a 14Gbps

#VamosPraticar#

(IFMG / IFMG – 2023) Qual o padrão IEEE está relacionado à tecnologia WI-FI 6?

- a) 802.11ac b) 802.11ax c) 802.11b d) 802.11g e) 802.11n

Comentários: o padrão conhecido Wi-Fi 6 é o 802.11ax (Letra B).

#VamosPraticar#

Assim como nas redes cabeadas, as Redes Wi-Fi (WLAN – Wireless LAN) também sofreram diversas evoluções. Observem a tabela apresentada acima: os padrões 802.11b e 802.11a surgiram simultaneamente, porém utilizaram tecnologias diferentes – **um não é evolução do outro**. O Padrão 802.11b entrou no mercado antes do Padrão 802.11a, se consolidando no mercado no início da década passada. Em seguida, veio o Padrão 802.11g...

Ele mantinha a compatibilidade com o Padrão 802.11b e precedia o Padrão 802.11n, que permitia maiores taxas de transmissão e operação em duas bandas de frequências (Dual Band). Por que, professor? Porque alguns aparelhos domésticos como controle de garagem, micro-ondas e bluetooth ^[14] trabalham na frequência de 2.4Ghz – isso poderia causar problemas de interferência. Como alternativa, ele pode trabalhar em outra frequência de onda de rádio!

Já o Padrão 802.11ac é uma novidade e pode vir a ser uma solução para tráfegos de alta velocidade, com taxas superiores a 1Gbps. Por fim, vejamos as principais vantagens e desvantagens:

Vantagens do padrão wi-fi	Desvantagens do padrão wi-fi
Permite conectividade sem fio, possibilitando o uso de dispositivos em movimento, como laptops e smartphones.	Redes sem fio estão suscetíveis a interferências de outros dispositivos e redes, afetando o desempenho.

Fácil instalação e expansão de redes sem fio, evitando a necessidade de cabos físicos.	As redes sem fio podem ser vulneráveis a invasões se as medidas de segurança, como criptografia, não forem implementadas adequadamente.
Geralmente mais econômico do que a instalação de cabos em locais com vários dispositivos.	A velocidade da rede sem fio pode ser mais lenta do que as redes com fio, especialmente em locais congestionados.
Oferece opções de configuração, como redes ad-hoc e infraestrutura, para atender a diversas necessidades.	A qualidade da conexão pode ser afetada por obstáculos físicos, distância do roteador e interferências.
Disponível em várias faixas de frequência, permitindo cobertura em diferentes distâncias.	Redes sem fio podem apresentar maior latência do que redes com fio, o que pode ser crítico para algumas aplicações.

Padrão Bluetooth (IEEE 802.15)



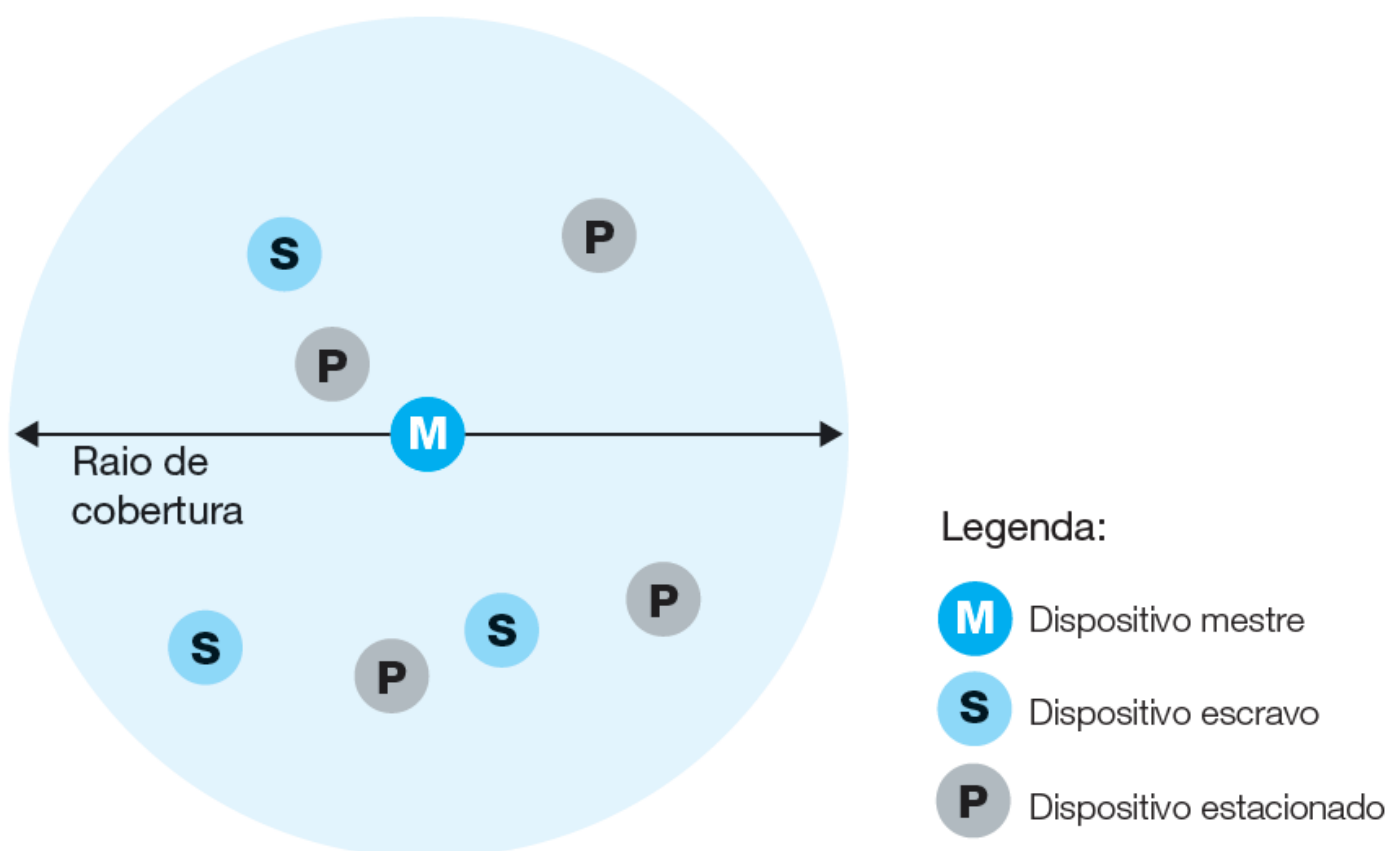
O Padrão Bluetooth tem o objetivo de integrar equipamentos periféricos.

Utilizado em Rede WPAN (Wireless Personal Area Network) – eles padronizam uma rede de baixo custo, curto alcance, baixas taxas de transmissão e sem fio. Eles operam na faixa de 2.4 Ghz de forma ad-hoc por meio de sua unidade básica: uma piconet. Também conhecida como picorrede ou pequena rede, trata-se de um grupo de dispositivos bluetooth que compartilham um canal comum de rádio-frequência.

Uma piconet possui uma topologia em estrela e uma configuração ou arquitetura do tipo Mestre-Escravo [15]. No centro dessa estrela, um dispositivo mestre (também chamado de *master* ou primário) coordena a comunicação com até outros sete dispositivos escravos (também chamados de *slave* ou secundários). Um dispositivo *bluetooth* pode desempenhar qualquer um dos papéis, mas em uma *piconet* só pode haver um dispositivo mestre.

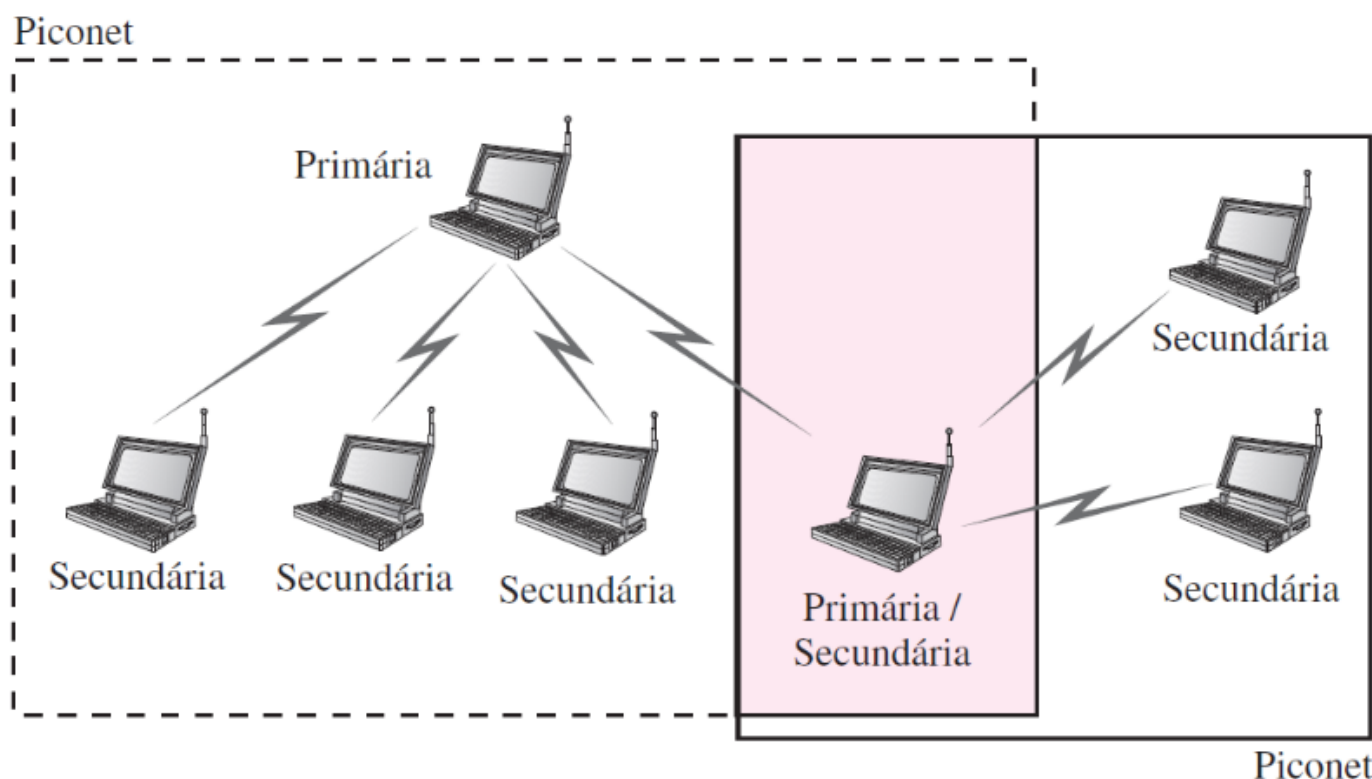
Além dos dispositivos escravos, a piconet também pode conter até 255 dispositivos estacionados. *Como assim, Diego?* Um dispositivo estacionado não pode se comunicar até que o dispositivo mestre altera seu estado de inativo para ativo. **Um dispositivo escravo que se encontre no estado estacionado permanece sincronizado com o mestre, porém não pode fazer parte da comunicação até deixar o estado estacionado.**

Como apenas oito estações podem estar ativas ao mesmo tempo em uma piconet, retirar uma estação do estado estacionado significa que uma estação ativa terá de ir para o estado estacionado. **Em suma, uma piconet é um conjunto de oito dispositivos: 1 mestre, até 7 escravos e até 255 estacionados.** Vejam na imagem seguinte um esquema em um dispositivo mestre tem um raio de cobertura com três dispositivos escravos e quatro dispositivos estacionados.



E se eu disser para vocês que um dispositivo pode ser escravo em uma piconet e mestre em outra piconet? **Pois é, quando redes piconets se combinam, forma-se uma scatternet.** Vejam no esquema abaixo que temos duas piconets em que cada uma possui apenas uma estação primária (ou mestre). Em rosa, há um dispositivo que é uma estação secundária (escrava) da piconet à esquerda e uma estação primária (mestre) da piconet à direita. Temos, portanto, uma scatternet :)

Vamos deixar um pouquinho a teoria de lado e ver um exemplo mais prático. Imagine que você está em seu churrasco de posse após ter passado no sonhado concurso público! Só que o *churras* está desanimado porque não está rolando música alguma. Você – então – decide conectar seu smartphone (dispositivo mestre) a uma caixinha de som (dispositivo escravo). Lembrando que o seu smartphone também pode estar sendo mestre de outros dispositivos.



Na minha casa, meu computador (mestre) forma uma piconet por estar conectado ao meu teclado, ao meu mouse e ao meu fone de ouvido (escravos). Por outro lado, meu smartphone (mestre) também está conectado ao meu fone de ouvido (escravo). **Logo, meu fone de ouvido é escravo em duas piconets diferentes. Agora vamos imaginar que o meu computador (mestre) também está conectado ao meu smartphone (escravo). Nesse caso, eu terei uma scatternet...**

Vamos resumir esses pontos: (1) uma piconet possui apenas um dispositivo mestre; (2) um dispositivo só pode ser mestre de uma piconet; (3) um dispositivo pode ser escravo de mais de uma piconet; (4) um dispositivo pode ser mestre de uma piconet e escravo de outra piconet; (5) mestres só se comunicam com escravos e escravos só se comunicam com mestres – não há comunicação direta entre escravos ou comunicação direta entre mestres.

PADRÃO BLUETOOTH – WPAN 802.15		
CLASSE	Potência	DISTÂNCIA
1	100 mW	Até 100 Metros
2	2.5 mW	Até 10 Metros

3	1 mW	Até 1 Metro
----------	------	-------------

Por fim, vejamos na tabela seguinte as vantagens e desvantagens do padrão IEEE 802.15, que podem variar dependendo da implementação específica e do contexto de uso:

Vantagens do padrão bluetooth	Desvantagens do padrão bluetooth
O padrão IEEE 802.15 é projetado para dispositivos de baixo consumo de energia, adequados para baterias.	As redes IEEE 802.15 têm alcance limitado, geralmente cobrindo apenas algumas dezenas de metros.
O padrão é ideal para comunicações de curto alcance, como sensores e dispositivos IoT em uma área próxima.	A largura de banda é limitada, o que a torna inadequada para aplicações que requerem alta taxa de transferência.
Permite a criação de redes de malha, onde dispositivos podem rotear dados entre si, aumentando a cobertura.	Pode ser afetada por interferências de outras redes sem fio e dispositivos, especialmente em ambientes lotados.
Usado em aplicações como IoT, sensores sem fio, automação residencial, dispositivos médicos e muito mais.	Não é a melhor opção para redes de grande escala, devido ao seu alcance limitado e limitações de largura de banda.
Substitui a necessidade de cabos em ambientes onde a conectividade com fio não é prática ou possível.	A segurança é uma preocupação, pois dispositivos dentro do alcance de uma rede IEEE 802.15 podem acessá-la.

Padrão WiMAX (IEEE 802.16)

INCIDÊNCIA EM PROVA: baixíssima

O Padrão WiMAX especifica um padrão sem fio de alta velocidade para Redes Metropolitanas (WMAN), criado por um consórcio de empresas para promover interoperabilidade entre equipamentos. Seu raio de comunicação com o ponto de acesso pode alcançar até cerca de 40 km, sendo recomendável para prover acesso à internet banda larga a empresas e residências em que o acesso ADSL ou HFC se torna inviável por questões geográficas.

#VamosPraticar#

(SELECON / IF-RJ – 2023) O IEEE (Institute of Electrical and Electronics Engineers) foi iniciado na década de 80 com o objetivo de elaborar padrões de rede, sendo responsável pela criação da arquitetura IEEE 802. A tecnologia WIMAX utiliza o padrão:

- a) 802.16
- b) 802.15
- c) 802.11
- d) 802.5
- e) 802.3

Comentários: a tecnologia WiMAX utiliza o padrão IEEE 802.16 (Letra A).

#VamosPraticar#

Opera em faixas licenciadas do espectro de frequência (2,5GHz, 3,5GHz, 10,5GHz), portanto é necessário que empresas adquiram a concessão junto à ANATEL (Agência Nacional de Telecomunicações) para oferecer esse serviço. A potência percebida na estação-base, que oferecerá o serviço, pode ter uma grande variação, o que influencia a relação sinal/ruído e, por isso, a tecnologia possui três esquemas de modulação (QAM-64, QAM-16 e QPSK).

Por fim, vejamos na tabela seguinte as vantagens e desvantagens do padrão IEEE 802.16, que podem variar dependendo da implementação específica e do contexto de uso:

Vantagens do padrão wimax	Desvantagens do padrão wimax
O IEEE 802.16 pode fornecer serviços de banda larga em uma ampla área	A implantação de infraestrutura 802.16 pode ser cara, especialmente em áreas com baixa

geográfica, incluindo áreas urbanas e rurais.	densidade populacional.
Oferece largura de banda significativa, o que é adequado para aplicações que exigem altas taxas de transferência de dados.	Apresenta latência mais alta em comparação com tecnologias como fibra óptica, o que pode afetar aplicativos sensíveis à latência.
Suporta mobilidade, permitindo a conexão de dispositivos em movimento, como em veículos ou trens de alta velocidade.	Pode ser suscetível a interferências de obstáculos, como edifícios altos e outros dispositivos sem fio na mesma faixa.
Comparado com tecnologias como DSL, o IEEE 802.16 pode oferecer conectividade de banda larga em áreas rurais remotas.	A compatibilidade entre diferentes implementações de 802.16 nem sempre é garantida, o que pode levar a problemas de interoperabilidade.
Oferece QoS para garantir que diferentes tipos de tráfego, como voz e vídeo, tenham desempenho adequado na rede.	A gestão eficaz do espectro é necessária para evitar interferências e garantir o desempenho da rede.

#VamosPraticar#

(VUNESP / Prefeitura de Birigui-SP – 2019) Assinale a alternativa que apresenta uma tecnologia de rede sem fio de longa distância.

- a) WiMAX.
- b) ZigBee.
- c) IEEE 802.11a.
- d) IEEE 802.11g.
- e) Bluetooth.

Comentários: a tecnologia que apresenta uma tecnologia de rede sem fio de longa distância é o WiMAX (Letra A).

#VamosPraticar#

1.9 Redes de Computadores - Parte 1 - Internet - Teoria

Internet

Conceitos Básicos

INCIDÊNCIA EM PROVA: média

A Internet é basicamente um vasto conjunto de redes de computadores diferentes que utilizam um padrão comum de comunicação e oferece um determinado conjunto de serviços. Hoje é muito comum o acesso à internet, mas vocês já pararam para pensar como tudo isso surgiu? Para entendê-la melhor, vamos contar um pouquinho dessa interessante história e vamos observar como e por que ela foi desenvolvida.

Tudo começa no final da década de 1950. Estávamos no auge da Guerra Fria entre EUA e URSS. Vocês se lembram qual era o maior medo daquela época? Lembrem-se que a 2ª Guerra Mundial havia acabado na década anterior com a explosão de uma bomba atômica. **Dessa forma, o Departamento de Defesa dos EUA decidiu que precisava de uma rede de controle e comando capaz de sobreviver inclusive a uma futura guerra nuclear com a União Soviética.**

Nessa época, a telefonia pública já era comum na vida das pessoas e todas as comunicações militares passavam por essa rede subterrânea de cabos de telefonia, mas ela era considerada vulnerável no caso de uma guerra. *Por que?* Porque essa rede funcionava de forma semelhante a uma arquitetura cliente/servidor – havia centrais telefônicas espalhadas por todo país. **Logo, bastava destruir algumas dessas centrais e toda comunicação telefônica seria interrompida.**

Em 1957, o mundo testemunhou um evento histórico para a humanidade: a União Soviética bateu os Estados Unidos na corrida espacial e lançou o primeiro satélite artificial do mundo – o Sputnik. O presidente americano Dwight Eisenhower ficou com muito medo de perder novas batalhas tecnológicas para o país rival e **criou uma organização única de pesquisas de defesa composta pelo Exército, Marinha e Aeronáutica chamada ARPA (Advanced Research Projects Agency).**

Na verdade, essa organização não possuía cientistas nem laboratórios – era basicamente um escritório. No entanto, ela era capaz de oferecer concessões e contratos a universidades públicas ou empresas que possuísem ideias promissoras, uma vez que se tratava de uma

agência de projetos de pesquisa avançada. **A ideia dessa organização era se manter sempre um passo à frente da União Soviética em tecnologia militar.**

Durante os primeiros anos, a agência financiou diversos projetos diferente, mas em determinado momento seu diretor – Larry Roberts – se encantou novamente com a ideia de uma rede de controle e comando. Em 1969, algumas poucas universidades importantes concordaram em ingressar no projeto e começou a construir essa rede. **Como se tratava de uma rede financiada pela ARPA, seu nome inicial foi ARPANET.**

Tudo começou bem pequeno, como um serviço de mensagens entre computadores da Universidade da Califórnia, Universidade de Stanford e a Universidade de Utah. Nas décadas seguintes, os cientistas e engenheiros adicionaram diversos outros recursos e serviços que ainda hoje compõem o que fazemos na Internet. **A primeira grande inovação da ARPANET foi a comutação por pacotes!** Vamos falar um pouco sobre comutação antes de seguir nossa história.



Antigamente havia um emprego que hoje em dia não existe mais: telefonista! *Quem aí já ouviu falar?* Pois é! Naquela época, quando alguém queria ligar para um amigo, era necessário ligar primeiro para uma central telefônica. Nesse local, havia centenas de operadoras que recebiam a sua ligação, perguntavam para quem você queria ligar, e só então conectavam você ao telefone do seu amigo. **Essa comunicação funcionava por meio da comutação por circuito!**

Professor, não entendi! Vamos observar com mais atenção a imagem! Temos cinco operadoras com fones de ouvido e microfones. Na frente delas, é possível ver um painel com pequenos

buracos e cabos plugados em alguns desses buracos. Em todo telefone, saía um cabo e passava por debaixo da terra por quilômetros e quilômetros até chegar a uma central telefônica. **Esses cabos que vocês estão vendo são os mesmos cabos conectados aos telefones residenciais.**

Pois bem... quando você queria telefonar para o seu amigo, você falava primeiro com a operadora por meio do cabo que saía da sua casa até a central telefônica. Ela perguntava com quem você queria falar e simplesmente plugava o cabo telefônico da sua casa ao cabo telefônico da casa do seu amigo. Pronto! **A partir desse momento vocês possuíam a reserva de um canal de comunicação dedicado e poderiam conversar sem interferências.**

É claro que se outra pessoa estivesse tentando te ligar, você não conseguiria atendê-la porque você está com o seu canal de comunicação ocupado/reservado. Pois bem... isso que nós acabamos de descrever se chama comutação por circuito. *Professor, o que significa esse termo comutação?* **No contexto de telecomunicações, é o processo de interligar dois ou mais pontos. No caso da telefonia, as centrais telefônicas comutam ou interligam terminais.**

Observem que a comutação por circuito estabelece um caminho fim a fim dedicado, reservando um canal de comunicação temporariamente, para que dados de voz sejam transmitidos. Nesse caso, a informação de voz sempre percorre a mesma rota e sempre chega na mesma ordem. **O processo de comutação por circuito possui uma fase de estabelecimento da conexão, uma fase de transferência de dados e uma fase de encerramento da conexão.**

Galera, eu vou contar uma coisa surpreendente para vocês agora! *Vocês acreditam que ainda hoje a telefonia funciona por meio da comutação de circuitos?* **Pois... é claro que não precisamos mais de operadores porque os circuitos são capazes de se mover automaticamente em vez de manualmente.** Legal, mas a comutação por circuito é completamente inviável na internet. *Por que, Diegão?* Cara, vamos lá...

O principal problema é o desperdício de recursos! **Poxa... quando um dispositivo de origem estabelece uma conexão com um dispositivo de destino, fecha-se uma conexão e ambas as linhas permanecem dedicadas mesmo que não esteja havendo comunicação.** Imaginem que eu estou falando com um amigo no telefone, mas estou apertado para ir ao banheiro! Se eu passar meia hora no banheiro, a linha continuará reservada mesmo sem eu estar utilizando.

Além disso, a comutação por circuito só permite que eu telefone para uma única pessoa simultaneamente – eu não consigo conversar com dois amigos simultaneamente. *Já imaginaram se a internet funcionasse assim?* Nesse caso, seu computador só poderia se conectar a um único dispositivo ao mesmo tempo. **Seria impossível acessar dois sites simultaneamente – você teria que fechar um site para poder acessar outro.**

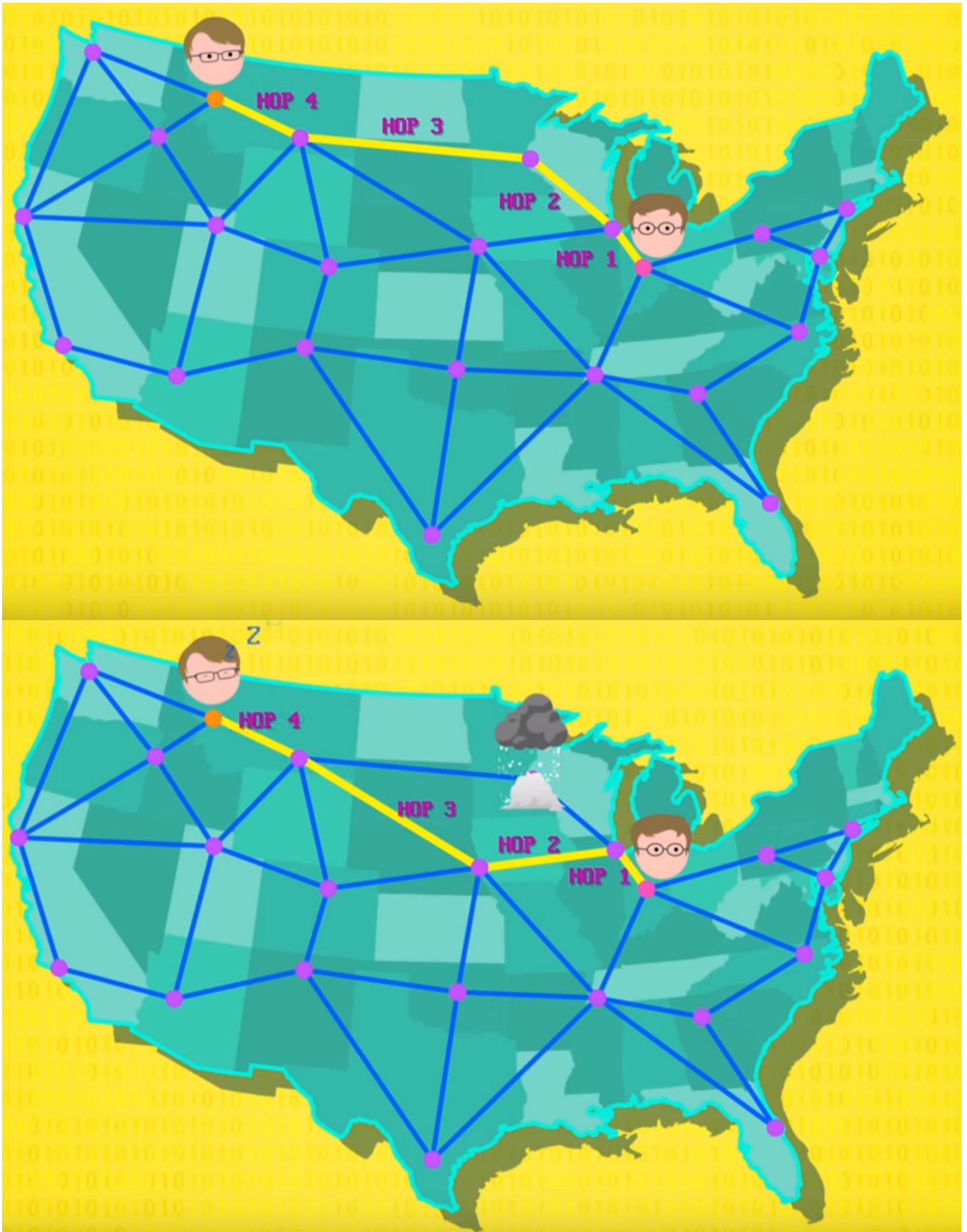
Além disso, o tráfego na internet é muito inconstante. Por exemplo: você começa a estudar uma aula de informática em nosso site, depois você sai para comer, depois você volta e entra em um site para ouvir uma música relaxante. *Vocês percebem que o perfil de utilização é totalmente diferente?* **Se utilizássemos a comutação por circuito na internet, você sairia para**

comer e deixaria a linha reservada mesmo sem a estar utilizando, desperdiçando recursos.



Algumas vezes, por questão de segurança ou por questão de relevância, é necessário manter uma linha exclusiva e dedicada. Por essa razão, forças armadas, bancos e outras organizações que possuem processos de alta criticidade mantêm linhas ou circuitos dedicados para conectar seus centros de dados como mostra a imagem anterior. **Voltando à história: a ARPANET trouxe um novo paradigma chamado Comutação por Pacotes.** Como funcionava?

Vamos falar uma analogia com uma empresa de entrega. Vamos supor que se John deseja enviar uma carta para David. **Em vez de ter uma estrada dedicada entre a cidade de John e a cidade de David, eles poderiam utilizar as diferentes rotas possíveis entre as duas cidades.** Exemplo: um caminhão poderia pegar a carta e transportá-la apenas de Indianápolis para *Chicago*. Ao chegar nessa cidade, ela poderia ir consultar a melhor rota e levaria de *Chicago* para *Minneapolis*.



Em seguida, a rota seria de *Minneapolis* para *Billings*; e finalmente de *Billings* até *Missoula* – como mostra a imagem abaixo à esquerda. Ao parar em cada cidade, o motorista do caminhão

poderia perguntar na estação de correio da cidade qual era a melhor rota até chegar ao destino final. **A parte mais interessante dessa abordagem é que ela pode utilizar rotas diferentes, tornando a comunicação mais confiável e tolerante a falhas.**

Como assim, professor? Imaginem que haja uma tempestade de neve na cidade de *Minneapolis* que congestionou absolutamente todas as vias. Não tem problema – o motorista do caminhão poderia utilizar outra rota passando por *Omaha* – como mostra a imagem acima à direita. **Voltando para o mundo das redes de computadores, não há necessidade de uma conexão estabelecer previamente uma rota dedicada para a transmissão de dados.**

Na comutação por pacotes, há uma malha de nós conectados ponto-a-ponto em que cada nó verifica a rota de menor custo para entrega da informação. *Como assim, Diego?* O caminho de menor custo é o caminho mais rápido entre dois pontos. Nas imagens anteriores, nós temos dois caminhos entre dois pontos. O primeiro é até mais curto, mas está congestionado – logo, o segundo caminho tem menor custo porque é o caminho mais rápido entre dois pontos.

Quem aí já usou o Waze? Por vezes, você já sabe o caminho entre seu trabalho e sua casa e você sabe que ele é o caminho mais curto. No entanto, ainda assim é interessante utilizar o Waze. *Por que?* Porque se houver um acidente no percurso, o caminho mais curto em distância pode ser mais lento em tempo do que eventualmente um caminho mais longo em distância. **O software sugerirá um caminho mais distante, mas que você chegará mais rápido.**

Agora tem outro ponto interessante sobre esse tipo de comutação! Por vezes, os dados transmitidos são grandes demais ao ponto de eventualmente obstruir uma rede completamente (Ex: envio de um arquivo de 100Mb). **A comutação por pacotes trouxe uma ideia genial: dividir as informações em pequenos pedaços chamados de pacotes.** Logo, em vez de enviar o arquivo integral, você o divide em milhares de pacotinhos. *O que tem de genial nisso, professor?*

Galera... se eu fragmento ou segmento uma informação em milhares de pacotes, eu posso enviá-los separadamente de modo que cada um possa percorrer uma rota totalmente diferente. *Professor, está muito complexo!* Vamos voltar ao exemplo dos correios: imagine que eu preciso enviar um relatório de 100 páginas para outro estado, mas que os correios só permitam o envio de 10 páginas por envelope.

Não tem problema! **Eu posso dividir meu relatório em dez pacotes de dez páginas e fazer dez envios diferentes.** Como os correios vão entregar os pacotes separadamente, cada pacote pode percorrer uma rota até o destino final. E digo mais: pode ser que as dez primeiras páginas cheguem por último e as últimas dez páginas cheguem primeiro. Cara... acontece quase igualzinho no contexto de internet.

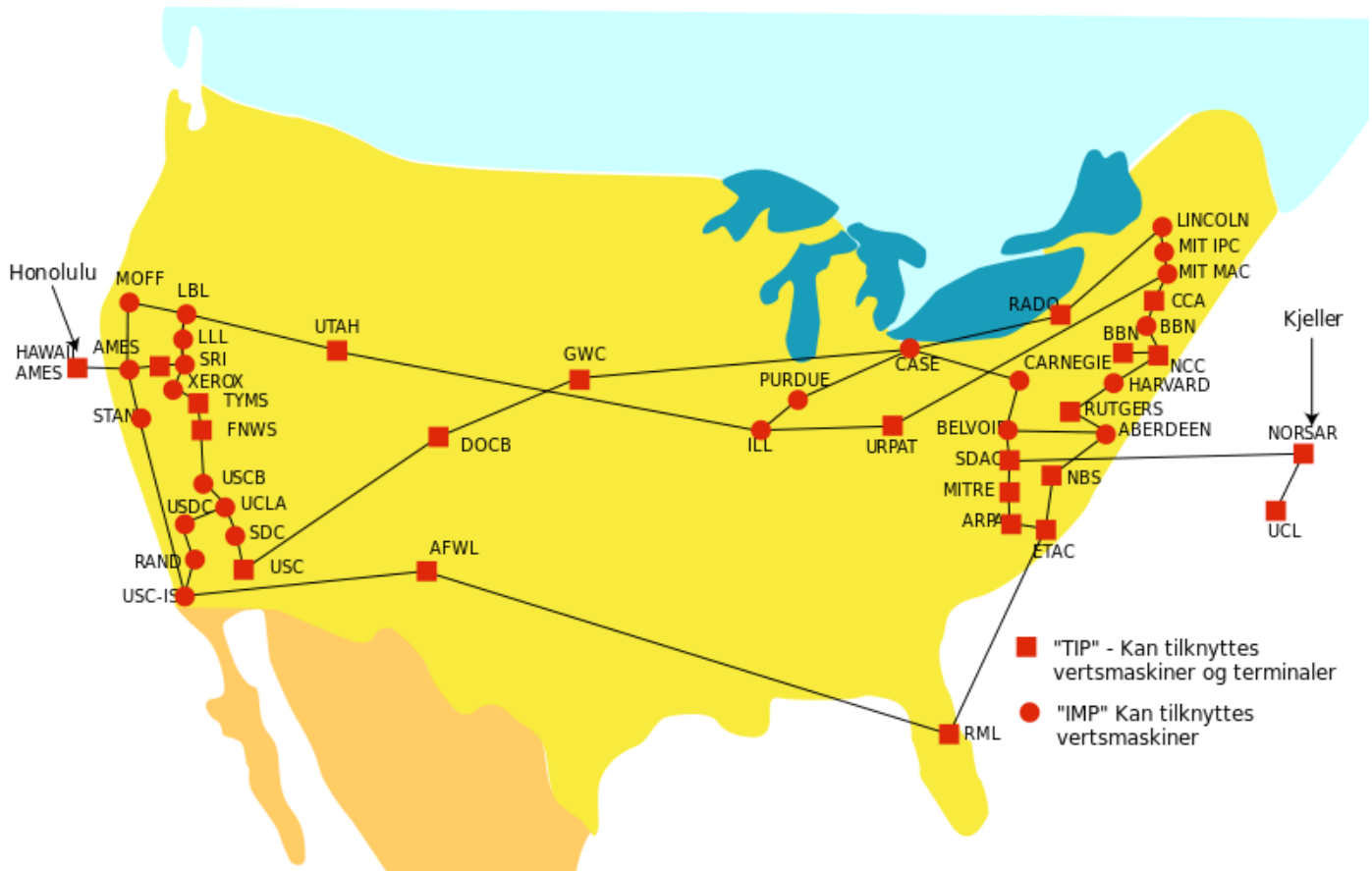
Quando se envia dados pela internet, não é possível prever o caminho percorrido pelo pacote até chegar ao seu destino final. Cada pacote enviado pode seguir por uma rota diferente chegando em ordem diferente da ordem enviada (claro que, após todos os pacotes chegarem, o arquivo é remontado na forma original). Pessoal, deixa eu contar uma coisa para vocês: nós só temos internet hoje em dia por conta dessa ideia genial...



A comutação por pacotes permite aproveitar melhor os canais de transmissão de dados de modo que sua utilização seja compartilhada pelos usuários da forma mais eficiente e tolerante a falhas possível. Ela utiliza um tipo de transmissão **store-and-forward**, em que o pacote recebido é armazenado por um equipamento e encaminhado ao próximo destino. Em cada equipamento, o pacote recebido tem um endereço de destino, que possibilita indicar o caminho final.

Pessoal... os engenheiros testaram a comutação por pacotes e foi um sucesso, mas – com o passar dos anos – a quantidade de novos computadores e dispositivos conectados à rede começou a aumentar e surgiu um problema. Nós vimos que o equipamento que recebe e armazena o pacote era responsável por encaminhá-lo ao próximo destino. No entanto, isso implicava que todo computador deveria manter uma lista **atualizada** do endereço de outros computadores da rede.

E se a lista não estivesse atualizada? Esse equipamento não saberia para onde enviar ou enviaria o pacote para um local que não existia mais, entre outras possibilidades. Com o aumento da quantidade de computadores na rede, era cada vez mais comum que computadores mudassem seu endereço e a atualização para os outros computadores da rede não era tão rápida. *Como eles resolveram esse problema, Diego?* Os caras eram sinistros...



Mapa da Arpanet em 1974

Em 1973, eles decidiram abolir esse sistema em que cada dispositivo possuía uma lista de endereços dos outros e escolheram a Universidade de Stanford como uma espécie de registro central oficial de endereços. Em 1978, já havia mais de cem computadores conectados à Arpanet por todo Estados Unidos e até Inglaterra. **Nos anos seguintes, começaram a surgir redes semelhantes à Arpanet em diferentes lugares do mundo com mais computadores.**

Legal, professor! É legal, mas originou alguns problemas. Cada rede criada formatava seus pacotes de maneira diferente, então – apesar de ser possível conectar redes diferentes – isso causava uma dor de cabeça. **Para resolver esse problema, a solução foi utilizar um conjunto de protocolos comuns de comunicação chamado TCP/IP.** O que é um protocolo, professor? Basicamente é uma convenção que controla e possibilita conexões, comunicações e transferências de dados.

Professor, você pode explicar de outra forma? **Claro, vamos fazer uma analogia!** Se eu comprar um notebook e ele vier com uma tomada de cinco pinos, eu não conseguirei utilizá-lo. Se ele funcionar em 110v, eu não conseguirei utilizá-lo em Brasília. Se eu comprar um mouse sem fio para utilizar com o notebook, mas eles operarem em faixas de frequência diferentes, eu também não conseguirei utilizá-los.

No primeiro caso, eu ainda posso comprar um adaptador; no segundo caso, eu ainda posso comprar um transformador; mas no terceiro caso, não há nada a se fazer. *O que vocês podem concluir de tudo isso?* É possível concluir que se os fabricantes de equipamentos não

conversarem entre si, haverá sérios problemas de comunicação de dados. **Por essa razão, foram criados protocolos comuns de comunicação, sendo o conjunto mais utilizado chamado de TCP/IP.**

Quando duas ou mais redes se conectam utilizando a pilha de protocolos TCP/IP, fica bem mais fácil conectá-las. O conjunto de redes de computadores que utilizam esses protocolos e que consiste em milhões de empresas privadas, públicas, acadêmicas e de governo, com alcance local ou global e que está ligada a uma grande variedade de tecnologias de rede é também conhecida popularmente como...

INTERNET

Atualmente, a internet oferece uma infinidade de serviços disponibilizados! Dentro os principais serviços, os mais conhecidos são:

SERVIÇOS	DESCRIÇÃO
World Wide Web (WWW)	Trata-se do serviço de visualização de páginas web organizadas em sites em que milhares de pessoas possuem acesso instantâneo a uma vasta gama de informação online em hipermídia que podem ser acessadas via navegador – é o serviço mais utilizado na Internet. Em geral, esse serviço utiliza protocolos como HTTP e HTTPS.
CORREIO ELETRÔNICO	Trata-se do serviço de composição, envio e recebimento de mensagens eletrônicas entre partes de uma maneira análoga ao envio de cartas – é anterior à criação da Internet. Utiliza tipicamente um modo assíncrono de comunicação que permite a troca de mensagens dentro de uma organização. Em geral, esse serviço utiliza protocolos como POP3, IMAP e SMTP.
ACESSO REMOTO	Trata-se do serviço que permite aos usuários facilmente se conectarem com outros computadores, mesmo que eles estejam em localidades distantes no mundo. Esse acesso remoto pode ser feito de forma segura, com autenticação e criptografia de dados, se necessário. Em geral, esse serviço utiliza protocolos como SSH, RDP, VNC.
TRANSFERÊNCIA DE ARQUIVOS	Trata-se do serviço de tornar arquivos disponíveis para outros usuários por meio de downloads e uploads. Um arquivo de computador pode ser compartilhado ou transferido com diversas pessoas através da Internet, permitindo o acesso remoto aos usuários. Em geral, esse serviço utiliza protocolos como FTP e P2P.

Esses são os serviços principais, mas existem muitos outros oferecidos via Internet (Ex: grupos de discussão, mensagens instantâneas, bate-papo, redes sociais, computação em nuvem, etc).

1.10 Redes de Computadores - Parte 1 - Gerações da Web - Teoria

Web (WWW)

INCIDÊNCIA EM PROVA: baixa

Web é uma contração do termo World Wide Web (WWW). *Ah, professor... você tá falando de internet, não é?* Não! Muito cuidado porque são coisas diferentes! **A internet é uma rede mundial de computadores que funciona como uma estrutura que transmite dados para diferentes aplicações.** A Web é apenas uma dessas aplicações – uma gigantesca aplicação distribuída rodando em milhões de servidores no mundo inteiro usando navegadores. Vejamos alguns exemplos:



Vamos entender isso melhor por meio de uma analogia: a Internet pode ser vista como uma vasta rede rodoviária que conecta cidades, estados e países. Essas estradas permitem que você vá de um lugar para outro, independentemente de qual seja o seu destino. Nessa rede rodoviária, você pode dirigir um carro, andar de bicicleta, caminhar, pegar um ônibus ou usar qualquer outro meio de transporte que desejar. **A estrutura das estradas e rodovias é o que torna tudo isso possível.**

Agora, pense na web como lojas, casas, escritórios e pontos de interesse que você encontra ao longo das estradas da Internet. Cada loja ou local representa um site da web, e você pode visitá-los para obter informações, fazer compras, se divertir, etc. Os sites da web são destinos ao

longo da estrada. Em suma: a web é composta por uma vasta coleção de documentos e recursos interconectados, que são acessados por **meio de navegadores da web**.

Componentes da web	DESCRIÇÃO
Hipertexto	A Web é baseada em documentos que contêm links (hiperlinks) para outros documentos relacionados. Isso permite que os usuários naveguem de uma página para outra, seguindo os links.
url	Cada documento ou recurso na Web é identificado por um URL exclusivo, que é um endereço usado para acessar o recurso em um navegador.
Navegadores da web	São aplicativos que permitem aos usuários visualizar e interagir com documentos da Web. Exemplos populares de navegadores incluem o Google Chrome, Mozilla Firefox, Microsoft Edge e Safari.
Protocolos de comunicação	A Web utiliza protocolos de comunicação, como HTTP (Hypertext Transfer Protocol) e HTTPS (HTTP Secure), para transferir dados entre navegadores e servidores web.
Servidores web	São computadores que hospedam documentos e recursos da Web. Eles respondem às solicitações dos navegadores e fornecem os conteúdos solicitados.
Páginas da web	São documentos criados usando linguagens de marcação, como HTML (Hypertext Markup Language). As páginas da web podem conter texto, imagens, links e outros elementos interativos.
Motores de busca	São ferramentas que ajudam os usuários a encontrar informações na Web, indexando e classificando páginas da web com base em palavras-chave.

(COTEC / Prefeitura de São Francisco-MG – 2020) Os termos internet e World Wide Web (WWW) são frequentemente usados como sinônimos na linguagem corrente, e não são porque:

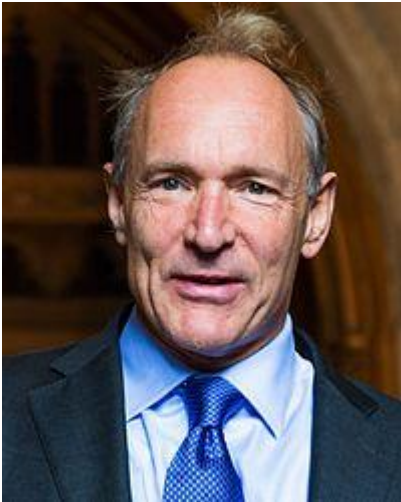
- a) a internet é uma coleção de documentos interligados (páginas web) e outros recursos, enquanto a WWW é um serviço de acesso a um computador.
- b) a internet é um conjunto de serviços que permitem a conexão de vários computadores, enquanto WWW é um serviço especial de acesso ao Google.
- c) a internet é uma rede mundial de computadores especial, enquanto a WWW é apenas um dos muitos serviços que funcionam dentro da internet.
- d) a internet possibilita uma comunicação entre vários computadores, enquanto a WWW, o acesso a um endereço eletrônico.
- e) a internet é uma coleção de endereços eletrônicos, enquanto a WWW é uma rede mundial de computadores com acesso especial ao Google.

Comentários: a internet é a infraestrutura de rede global que conecta computadores em todo o mundo, enquanto a World Wide Web (WWW) é um serviço específico dentro da internet que permite o acesso a documentos interligados (páginas web) e outros recursos por meio de navegadores da web. A WWW é apenas uma parte dos muitos serviços e recursos disponíveis na internet (Letra C).

#VamosPraticar#

Web 0.0

Em março de 1989, a World Wide Web teve a primeira especificação composta pelo Protocolo HTTP e a Linguagem HTML lançada por Tim Berners-Lee. Sim, se utilizamos a web atualmente, devemos agradecer a esse senhor aqui do lado! Até então, a web era uma fonte de acesso a informações, onde páginas de hipertexto (textos com links), de conteúdo estático, escritas por jornalistas e outros profissionais eram publicadas em Servidores Web e podiam apenas ser lidas pelos demais usuários. *Galera, vocês querem conhecer a primeira página web da história?* Segue o link abaixo:



<http://info.cern.ch/hypertext/WWW/TheProject.html> ^[16]

Em 1991, a página web acima era a única do mundo; em 1994, já havia 2.738 páginas web – inclusive o **Yahoo!**; em 1998, já havia 2.410.067 páginas web – inclusive o **Google**; em 2001, já havia 29.254.370 páginas web – inclusive a **Wikipedia**; em 2005, já havia 64.780.617 páginas web – inclusive o **Youtube** em 2008, já havia 172.338.776 páginas web – inclusive o **Dropbox**; e em 2018, temos 1.805.260.010 páginas web – inclusive o **Estratégia Concursos**!

World Wide Web

The WorldWideWeb (W3) is a wide-area [hypermedia](#) information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an [executive summary](#) of the project, [Mailing lists](#), [Policy](#), November's [W3 news](#), [Frequently Asked Questions](#).

[What's out there?](#)

Pointers to the world's online information, [subjects](#), [W3 servers](#), etc.

[Help](#)

on the browser you are using

[Software Products](#)

A list of W3 project components and their current state. (e.g. [Line Mode](#), [X11 Viola](#), [NeXTStep](#), [Servers](#), [Tools](#), [Mail robot](#), [Library](#))

[Technical](#)

Details of protocols, formats, program internals etc

[Bibliography](#)

Paper documentation on W3 and references.

[People](#)

A list of some people involved in the project.

[History](#)

A summary of the history of the project.

[How can I help?](#)

If you would like to support the web..

[Getting code](#)

Getting the code by [anonymous FTP](#), etc.

Web 1.0

A Web 1.0 refere-se à primeira geração da World Wide Web, **que se originou nos anos 90 e durou até o início dos anos 2000**. Ela foi caracterizada por vários elementos distintos:

CARACTERÍSTICAS DA WEB 1.0	DESCRIÇÃO
Estática e Somente Leitura	Sites da Web 1.0 eram predominantemente estáticos e unidirecionais. Eles consistiam principalmente em páginas HTML simples, que ofereciam informações estáticas aos visitantes. Os usuários podiam apenas ler o conteúdo e não interagir de forma significativa com o site.
CONTEÚDO LIMITADO	O conteúdo disponível na Web 1.0 era limitado à publicação de texto e imagens. Vídeos, áudios e outros formatos de mídia não eram comuns.
Falta de interatividade	Não havia recursos avançados de interatividade. Os visitantes podiam, no máximo, clicar em links para navegar entre páginas e preencher formulários de contato simples.
Uso limitado de tecnologia	A tecnologia subjacente era principalmente HTML, com poucas opções para dinamizar o conteúdo da web. Não havia ferramentas avançadas de desenvolvimento web, como APIs (Interfaces de Programação de Aplicativos) ou tecnologias AJAX.
Falta de redes sociais e colaboração	Redes sociais como as conhecemos hoje não existiam na Web 1.0. A interação social on-line era limitada, e não havia plataformas de compartilhamento de conteúdo ou colaboração em tempo real.
Busca ineficiente	Os mecanismos de busca eram primitivos e muitas vezes geravam resultados imprecisos. A indexação de conteúdo era baseada em palavras-chave, o que tornava a busca menos eficaz.

Era da informação	A Web 1.0 era predominantemente uma fonte de informações. Os sites eram usados para publicar informações sobre empresas, instituições, produtos e serviços, mas havia pouca ênfase na interação ou na criação de conteúdo pelos usuários.
Marcas e empresas	A Web 1.0 foi dominada por empresas e marcas que criaram sites institucionais para fornecer informações sobre si mesmas e seus produtos.

Imagine a Web 1.0 como uma grande biblioteca virtual. Nessa biblioteca, você pode encontrar uma enorme quantidade de livros e revistas, mas eles são todos impressos e não podem ser alterados. Você pode navegar pelos corredores, pegar um livro e lê-lo, mas não pode escrever ou adicionar suas próprias anotações nos livros. A biblioteca é um recurso de leitura valioso, mas é estática, sem interatividade.

Nesse cenário, as empresas e instituições são como os curadores da biblioteca, selecionando e disponibilizando informações para os visitantes. Os visitantes podem encontrar informações úteis, mas não têm a capacidade de contribuir com seu próprio conteúdo ou interagir com outros visitantes. **A Web 1.0 é semelhante a essa biblioteca digital, onde o conteúdo é fornecido para leitura, mas não há recursos avançados de interatividade, colaboração ou personalização.**

#VamosPraticar#

(QUADRIX / CREF3 – 2023) A web 1.0 é a terceira fase da web, que está sendo vivenciada hoje: ela é marcada pelo uso da inteligência artificial, para que os computadores executem, de forma automática, funções que antes seriam executadas pelo usuário.

Comentários: a descrição apresentada na afirmação não corresponde à Web 1.0. A Web 1.0 é, na verdade, a primeira fase da web, que se estendeu até meados dos anos 2000. Nessa fase, a web era caracterizada principalmente pela apresentação de informações estáticas e não interativas. Não havia um uso generalizado de inteligência artificial para automação de funções. A afirmação se assemelha mais à descrição da Web 3.0, que se refere à web semântica e à automação inteligente de tarefas por meio de máquinas e algoritmos (Errado).

#VamosPraticar#

Web 2.0

A Web 2.0 se refere a uma internet mais **dinâmica**, **interativa** e **colaborativa**, onde os usuários desempenham um papel central na criação e compartilhamento de conteúdo. Vejamos:

CARACTERÍSTICAS DA WEB 2.0	DESCRIÇÃO
INTERATIVIDADE	Os sites e aplicativos da Web 2.0 oferecem uma experiência mais interativa para os usuários. Eles podem deixar comentários, avaliações, compartilhar conteúdo e até mesmo contribuir com suas próprias informações. Plataformas como redes sociais, blogs, wikis e fóruns permitem que as pessoas se envolvam ativamente.
CONTEÚDO GERADO PELO USUÁRIO	Os usuários não são mais apenas consumidores de conteúdo; eles são produtores ativos. Eles criam blogs, carregam vídeos, compartilham fotos e colaboram em wikis. Plataformas como Youtube, Wikipedia e WordPress são exemplos disso.
REDES SOCIAIS	As redes sociais desempenham um papel fundamental na Web 2.0. Elas conectam pessoas, permitindo que compartilhem informações, conversem e construam relacionamentos online. Exemplos incluem Facebook, Twitter, LinkedIn e Instagram.
COLABORAÇÕES	A colaboração é promovida por meio de ferramentas que permitem que várias pessoas trabalhem juntas em projetos, como Google Docs ou sistemas de gerenciamento de projetos online.
PERSONALIZAÇÃO	A Web 2.0 oferece serviços mais personalizados, adaptando o conteúdo com base nas preferências do usuário. Isso é visível em recomendações de produtos da Amazon, playlists personalizadas do Spotify e anúncios direcionados do Google.

MASH-UPS	A capacidade de combinar dados e funcionalidades de diferentes fontes é uma característica da Web 2.0. Os desenvolvedores podem criar aplicativos que agregam informações de várias fontes, como mapas do Google que mostram informações do tráfego em tempo real.
WEB SEMÂNTICA	Embora em desenvolvimento, a Web Semântica é uma parte importante da visão da Web 2.0. Envolve a criação de um ambiente onde as máquinas podem entender o conteúdo da web, tornando-o mais significativo e útil para os usuários.

Imagine a Web 2.0 como uma biblioteca em que você não apenas lê os livros, mas pode adicionar seus próprios capítulos, comentários e até mesmo escrever seus próprios livros. Além disso, você pode se conectar com outros leitores, discutir ideias, fazer recomendações e criar novas histórias juntos. É como se a biblioteca se transformasse em um espaço de colaboração ativa, onde todos são autores e leitores ao mesmo tempo.

Da mesma forma, a Web 2.0 permitiu que os usuários não apenas consumissem informações, mas também as criassem, compartilhassem e colaborassem em um ambiente online, tornando a internet mais interativa e participativa. **É uma mudança de uma web estática e informativa para uma web dinâmica e social, onde os usuários desempenham um papel ativo na criação e compartilhamento de conteúdo.**

Web 3.0

A Web 3.0 é uma evolução da World Wide Web que visa tornar a internet **mais inteligente** e capaz de **compreender o conteúdo que está disponível online**. Vejamos suas principais características:

CARACTERÍSTICAS DA WEB 3.0	DESCRIÇÃO
semântica	A Web 3.0 se concentra em adicionar metadados semânticos aos dados, permitindo que as máquinas compreendam melhor o conteúdo. Isso significa que os computadores podem entender o significado dos dados, em vez de simplesmente processar texto e números.

Inteligência artificial	A IA desempenha um papel fundamental na Web 3.0. Máquinas e algoritmos podem aprender, raciocinar e tomar decisões com base nos dados disponíveis.
Conectividade	A Web 3.0 visa criar uma rede de informações altamente conectada, onde os dados podem ser relacionados e combinados de maneira mais inteligente. Isso facilita a recuperação de informações relevantes.
Personalização	A personalização é uma parte importante da Web 3.0. Os sistemas podem entender as preferências do usuário e fornecer conteúdo adaptado às necessidades individuais.
Interoperabilidade	A Web 3.0 se esforça para tornar os dados e serviços interoperáveis, de modo que diferentes aplicativos e sistemas possam funcionar juntos de maneira eficaz.
Web semântica	A Web Semântica é uma iniciativa importante na Web 3.0. Ela envolve a marcação de dados com metadados semânticos para que as máquinas possam entender as relações e conexões entre diferentes conjuntos de dados.
Aplicações diversificadas	A Web 3.0 tem aplicações em várias áreas, como comércio eletrônico, assistentes virtuais, pesquisa avançada, automação residencial, cuidados com a saúde, cidades inteligentes e muito mais.

Agora, a biblioteca é inteligente o suficiente para entender o conteúdo de cada livro. Ela sabe o enredo, os personagens, as informações-chave e como os livros se relacionam uns com

os outros. Quando você faz uma pergunta ao bibliotecário, ele não apenas recomenda os livros certos, mas também pode dizer coisas como *"Há um livro que menciona isso que você está procurando na seção de história, mas também pode estar relacionado à política na seção de não ficção"*.

A biblioteca está interconectada e usa inteligência artificial para fornecer informações significativas instantaneamente. Então, na analogia, a Web 1.0 é como uma biblioteca sem catálogo, a Web 2.0 é como uma biblioteca com etiquetas e um bibliotecário eficiente, e a Web 3.0 é como uma biblioteca ultra-inteligente que compreende o conteúdo de todos os livros e fornece respostas detalhadas com base em seu conhecimento profundo.

Características	Web 1.0	Web 2.0	Web 3.0
Interatividade	Baixa	Alta	Muito Alta
conteúdo	Estático e somente leitura	Dinâmico, com feedback do usuário	Inteligente, com semântica
Usuários	Consumidores passivos	Produtores de conteúdos	Participantes ativos
Socialização	Ausente	Integração de redes sociais	Integração com IA e Internet das Coisas
Experiência do usuário	Limitada	Melhorada e personalizada	Altamente personalizada
Tecnologia	HTML	AJAX, APIs e RSS	IA e Aprendizado de Máquina
Exemplos	Sites estáticos de início da web	Redes sociais, blogs e wikis	Assistentes virtuais

Principais aplicações	Sites informativos e institucionais	Redes sociais e colaboração online	Assistentes virtuais e Internet das Coisas

#VamosPraticar#

(CEPUERJ / UERJ – 2022) A Web 3.0 é identificada como web:

- a) pragmática
- b) semântica
- c) semiótica
- d) ubíqua

Comentários: a Web 3.0 é conhecida como Web Semântica, dado que – nessa fase – os sistemas de computação têm a capacidade de entender o significado dos dados e relacioná-los de maneira mais eficaz (Letra B).

#VamosPraticar#

1.11 Redes de Computadores - Parte 1 - Deep Web e Dark Web - Teoria

Deep Web e Dark Web

INCIDÊNCIA EM PROVA: média

Galera, vamos falar agora sobre um assunto que interessa grande parte dos alunos! *Qual seria a sua reação se eu te dissesse que tudo que você conhece sobre a web é, na verdade, apenas 4% da realidade?* Sim, todos os sites que você já visitou, todos os vídeos que você já assistiu, todas as músicas que você já ouviu, todos os textos que você já leu, todas as notícias que você já, todo material do Estratégia, Google, Wikipedia, etc... **tudo isso corresponde somente a cerca de 4% da web!**



Nós podemos dizer que a parte da web que pode ser indexada por **Ferramentas de Busca** (Ex: Google, Bing, etc) de modo que seja visível e acessível diretamente por navegadores comuns **sem a necessidade de autenticação** (Ex: Login e Senha) é chamada de **Surface Web (Superfície da Web ou Web Navegável)**. Você só encontra a página do Estratégia no Google porque ele possui rastreadores que ficam circulando pela web procurando páginas e

inserindo-as em um índice.

Características	Descrição
Acessibilidade	Facilmente acessível por meio de mecanismos de busca e navegadores padrão.
Conteúdo público	Compreende sites, páginas e conteúdo que são acessíveis ao público em geral.
Indexação por mecanismos de busca	Os motores de busca, como Google e Bing, indexam e exibem o conteúdo da Surface Web em resultados de pesquisa.
Informações amplamente visíveis	Notícias, blogs, lojas online, fóruns públicos e outros tipos de sites podem ser encontrados na Surface Web.
Sem restrições significativas	Os usuários podem navegar e acessar conteúdo sem a necessidade de credenciais ou permissões especiais.
exemplos	Páginas de notícias, blogs, lojas online e outros sites acessíveis ao público em geral.

Logo, tudo que ele consegue indexar (isto é, inserir em seu índice de pesquisa) são as páginas da web navegável. *E onde é que estão os outros 96%? **Estão na Deep Web (Web Profunda)**!* Lá está a parte da web que está protegida por mecanismos de autenticação ou que não pode ser acessada por meio de links tradicionais ou ferramentas de buscas, tais como seus e-mails ou sua conta no Internet Banking. *Uma página aberta no Facebook? Surface Web! Um grupo fechado? Deep Web!*

A Deep Web é invisível para todos aqueles que não tenham autorização para acessá-la. *Como assim, professor? Vamos imaginar a Intranet do Senado Federal! Você consegue acessá-la?* Em princípio, não – a não ser que você seja um servidor desse órgão! Dessa forma, podemos afirmar que a Intranet do Senado Federal está na Deep Web (apesar de esse ser um assunto bem polêmico)! **Agora faz sentido para você que a maioria dos dados estejam na Deep Web e, não, na Surface Web...**

No entanto, estar na Deep Web não é nenhuma garantia inquebrável de privacidade. Toda vez que acessamos uma página por meio de um navegador comum, nosso computador se comunica com o servidor que armazena a página que desejamos acessar. Essa conexão entre computador e servidor percorre uma rota que passa por diversos intermediários ao redor do planeta, deixando rastros quem podem ser utilizados para descobrir quem está acessando e o que está acessando.

Características	Descrição
Conteúdo não indexado por motores de busca	O conteúdo da Deep Web não é indexado pelos mecanismos de busca tradicionais, o que o torna invisível nas pesquisas comuns.
Requer autenticação	Muitos sites da Deep Web exigem credenciais ou autenticação para acessar, tornando o conteúdo acessível apenas a usuários autorizados.
Informações confidenciais	Inclui informações privadas, como dados de empresas, registros médicos, sistemas de gerenciamento de bibliotecas e muito mais.
Não acessível por links comuns	Você não pode simplesmente clicar em um link para acessar o conteúdo da Deep Web; geralmente, precisa de informações de login ou URLs específicas.
Variedade de conteúdo	A Deep Web abrange uma ampla gama de informações, desde bancos de dados privados a sistemas de gerenciamento de conteúdo corporativo.

Vocês se lembram quando um juiz tentou bloquear o acesso ao Whatsapp por 72 horas? Pois é, seu intuito era obrigar a empresa a quebrar o sigilo das mensagens trocadas por criminosos. E qual é o problema de bloquear um serviço, professor? **O problema é que – se é possível fazer isso por motivos legítimos – também é possível fazer isso ilegítimos.** A China, por exemplo, proíbe seus cidadãos de acessarem o Google, Facebook, Youtube, Twitter, etc.



19/07/2016 11h28 - Atualizado em 19/07/2016 17h08

WhatsApp: Justiça do RJ manda bloquear aplicativo em todo o Brasil

Facebook recusou ceder informações para uma investigação policial.
Operadoras de telefonia foram notificadas para suspender acesso ao app.

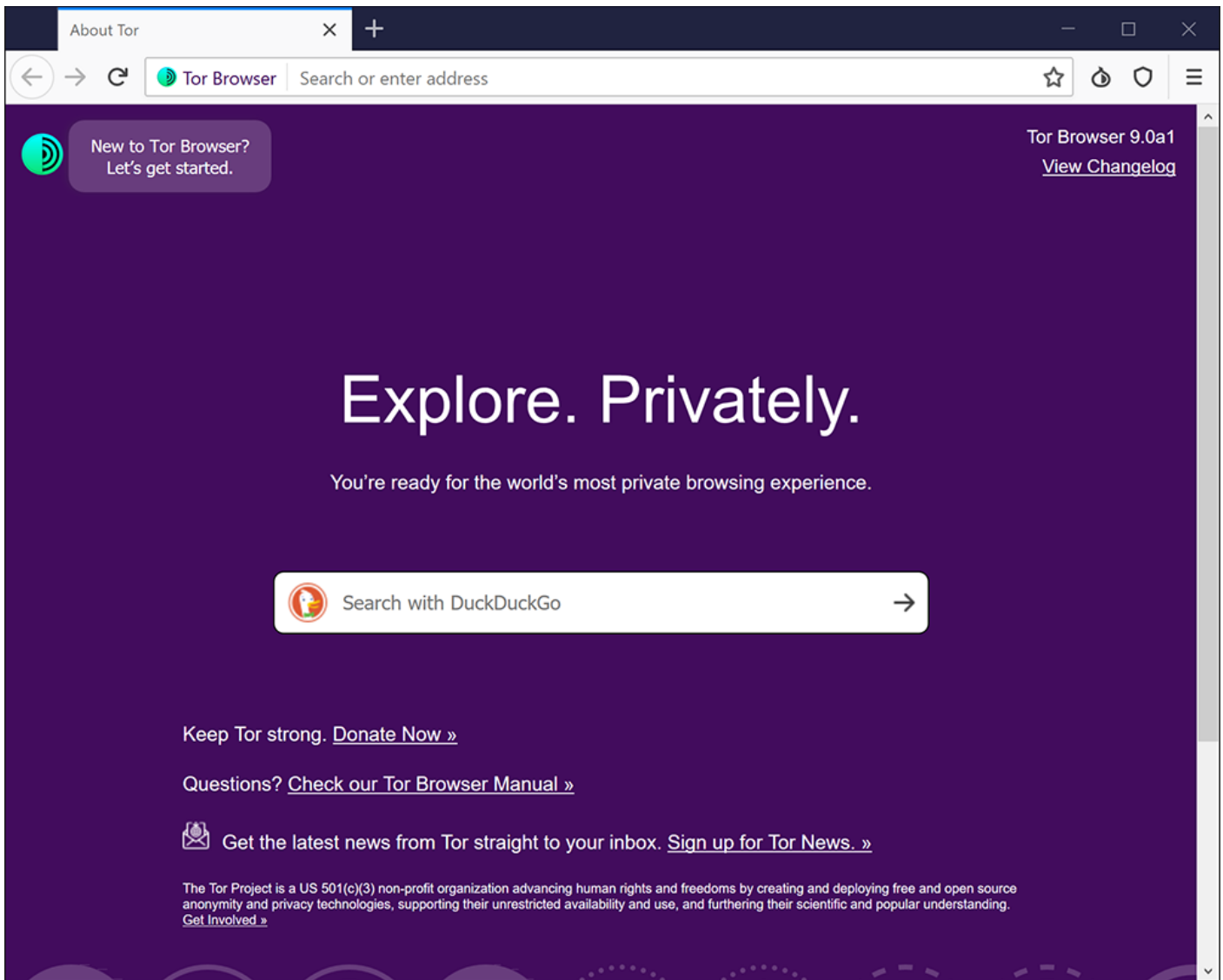
Do G1, em São Paulo e no Rio



Essa falta de privacidade pode ser um problema gravíssimo para cidadãos que vivem em países com censura, jornalistas, informantes, ativistas e até usuários comuns. Caso essas pessoas façam alguma crítica ao governo na Surface Web, elas podem eventualmente ser rastreadas e perseguidas por agentes governamentais. **Logo, os recursos da Deep Web permitem que ela possa manter sua privacidade e ter sua identidade preservada.** E o que elas podem fazer?

Bem, uma alternativa é utilizar a Dark Web! Trata-se de uma parte da Deep Web que não é indexada por mecanismos de busca e nem possuem um endereço comum ^[17], logo é basicamente invisível e praticamente impossível de ser rastreada. **Para acessá-la, é necessário se conectar a uma rede específica – a mais famosa se chama Tor.** Essa rede foi inicialmente um projeto militar americano para se comunicar sem que outras nações pudessem descobrir informações confidenciais.

Eita, professor... deixa eu acessar rapidinho aqui essa tal de Rede Tor! Nope, você não conseguirá! A Dark Web não é acessível por meio de navegadores comuns, tais como Chrome, Firefox, entre outros (exceto com configurações específicas de proxy). Para acessar a Rede Tor, é necessário utilizar um navegador específico – **também chamado de Tor** – que permite acessar qualquer página da Surface Web, Deep Web ou Dark Web (aliás, é assim que chineses conseguem acessar o Google).



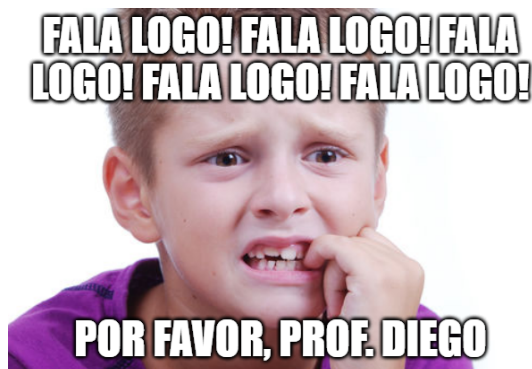
O Navegador Tor direciona as requisições de uma página através de uma rota que passa por uma série de servidores proxy da Rede Tor operados por milhares de voluntários em todo o mundo, **tornando o endereço IP não identificável e não rastreável** [18]. Vocês não precisam entender como isso funciona, vocês só precisam entender que os dados passam por uma série de camadas de encriptação de modo que seja praticamente impossível identificar de onde veio a requisição.

Características	Descrição
Acessível com software específico	A Dark Web é acessada por meio de redes criptografadas, como o Tor (The Onion Router), que requerem software especial para acesso.
Conteúdo ilegal e obscuro	Inclui sites que hospedam atividades ilegais, como tráfico de drogas, armas, venda de informações roubadas e outros conteúdos obscuros.

Anonimato é valorizado	Os usuários da Dark Web muitas vezes valorizam o anonimato, pois os serviços são frequentemente anônimos e transações são criptografadas.
Riscos à segurança	A Dark Web é um ambiente de alto risco, onde os usuários podem ser vítimas de fraudes e ataques cibernéticos.
Níveis mais profundos de anonimato	Diferentemente da Deep Web, a Dark Web oferece um nível mais profundo de anonimato e criptografia, tornando difícil rastrear usuários.

Conforme eu disse anteriormente, pode-se acessar páginas da Surface Web por meio desse navegador. Nesse caso, não é possível identificar quem está acessando, mas é possível identificar qual serviço está acessando (Ex: Google). Por outro lado, há algumas páginas da Dark Web que realmente só existem dentro da Rede Tor. Nesse caso, é absolutamente impossível identificar quem está acessando, quando está acessando, o que está acessando, etc – é completamente anônimo.

Professor, você disse que as pessoas acessam a Dark Web por motivos legítimos e ilegítimos. Eu estou agoniado, desembucha logo e fala o que é que tem de ilegítimo lá!



Galera, você pode encontrar usuários negociando entorpecentes e armas, contratando matadores de aluguel, planejando atentados terroristas, enviando vídeos de suicídio, compartilhando fotos de pedofilia, vazando documentos de empresas ou governos, trocando fotos de nudez, exibindo fotos/vídeos de torturas, estupro e homicídios de pessoas e animais, conteúdos racistas e xenófobos, canibalismo, esquisitices, falsificação de documentos, entre outros.

Eu sei que essa aula atiga a curiosidade de várias pessoas, mas eu já adianto que não recomendo que vocês acessem esses sites. Saibam que se trata de um ambiente em que é possível encontrar um bocado de hackers, cibercriminosos e outros profissionais desse tipo. Eu já recebi perguntas de alunos perguntando sobre “hipóteses” de atividades não muito legítimas. **Para terminar, vamos apenas falar um pouco sobre a relação entre a Dark Web e Criptomoedas.**

Em 2013, havia uma página na Rede Tor – chamada Silk Road – que vendia de tudo (desde metanfetaminas à discografia do Michael Jackson). *Professor, como havia vendas? Colocar o cartão de crédito não deixaria rastros?* Não eram utilizados cartões de créditos – era utilizado

uma criptomoeda (moeda virtual/digital) chamada Bitcoin. **Essa moeda virtual não passa pelo sistema financeiro nacional dos países e, quando usada em uma Rede Tor, não pode ser rastreada.**

Por meio dessa moeda, é possível comprar produtos e serviços. Só para que vocês saibam como não é possível ficar totalmente anônimo, o dono desse site (imagem acima) vacilou e fez uma pergunta utilizando seu nome verdadeiro em um fórum de programadores da Surface Web. O FBI já estava o investigando por conta de outras atividades ilícitas, acabou ligando os pontos **e ele foi preso e condenado a duas sentenças de prisão perpétua + 40 anos e sem liberdade condicional.**



Welcome **OzFreelancer!**
messages(0) | orders(0) | account(**80.00**) | settings | log out

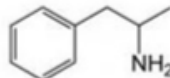
search | **(0)**

Shop by category:

Drugs(1582)
Cannabis(271)
Dissociatives(33)
Ecstasy(217)
Opioids(106)
Other(65)
Prescription(274)
Psychedelics(306)
Stimulants(190)
Apparel(37)
Art(1)
Books(300)
Computer
equipment(9)
Digital goods(218)
Drug
paraphernalia(33)
Electronics(13)



10 Grams high grade
MDMA 80+%
\$61.17



Amphetamines sulfate /
Speed freebase...
\$28.59



2g Jack Frost (weed) *420
SALE****
\$8.54



5 Grams of pure MDMA
crystals
\$42.04



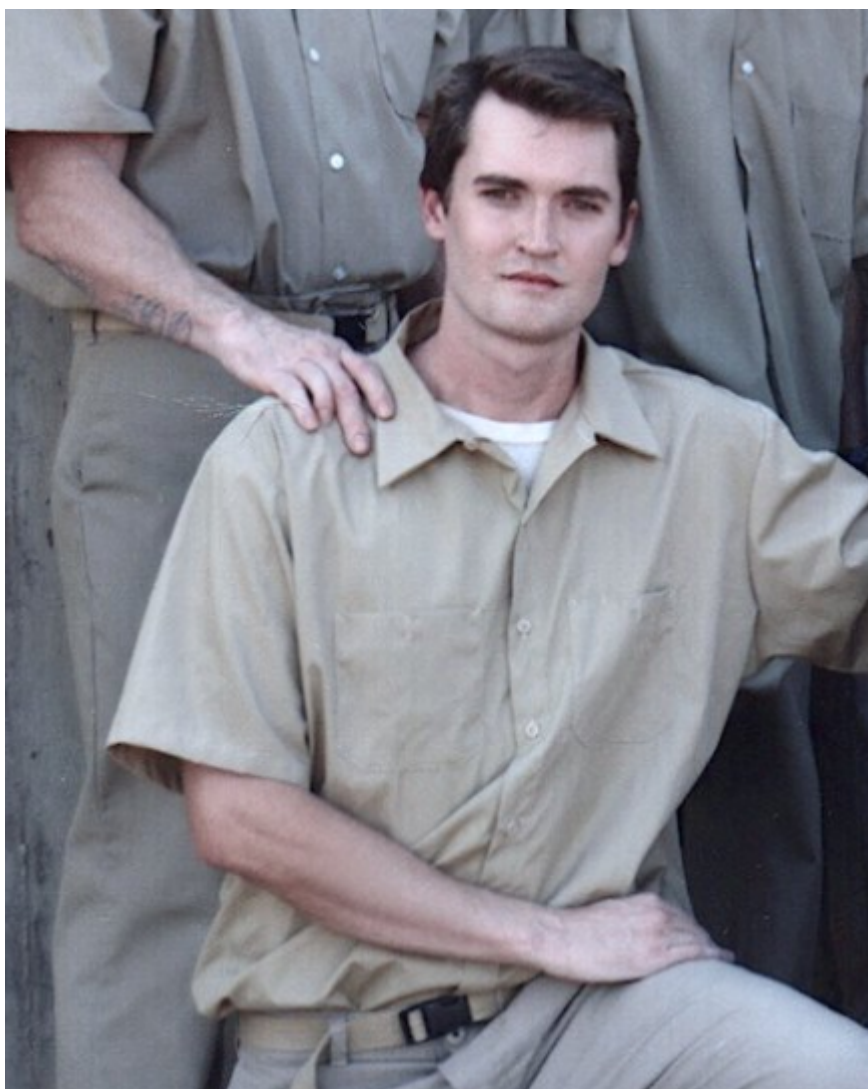
100 red Y tablets 111mg
(lab tested)...
\$97.77



Michael Jackson
Discography 1971-2009...
\$2.52

News:

- The gift that keeps on **giving**
- Who's your **favorite?**
- Acknowledging **Heroes**
- A new anonymous market **The Armory!**
- **State of the Road Address**



Um outro caso que vocês devem estar familiarizados é o Massacre de Suzano. Em 2019, dois ex-alunos de uma escola entraram armados nessa escola, mataram cinco estudantes e duas funcionárias – depois um dos atiradores matou o comparsa e, em seguida, cometeu suicídio. Os dois atiradores organizaram o crime em um fórum da Dark Web chamado Dogolochan – eles foram incitados por outros usuários e entraram na “Galeria de Ídolos” do fórum com outros criminosos.

Fóruns na dark web incitam violência e mortes e desafiam polícia

Massacre em Suzano foi comemorado em comunidades virtuais de criminosos



Luiz tinha 25 anos e era conhecido no fórum como "luhkrcher666"; Guilherme tinha 17 anos e era conhecido no fórum como "1guY-55chaN". Bem, esse é um assunto ainda bastante incipiente em concurso público, mas que deve ganhar importância nos próximos anos. Quem estiver curioso e quiser descobrir mais detalhes sobre esse assunto, recomendo dois documentários: **Dark Web (2015)** e **Don't F**k With Cats (2019)** – esse segundo está na Netflix :)

Por fim, vamos resumir tudo o que vimos na tabela apresentada a seguir e, por fim, uma analogia para finalmente consolidar o entendimento sobre esse conteúdo.

Características	Surface web	Deep web	Dark web
Acessibilidade	Acessível por mecanismos de busca e navegadores comuns.	Requer credenciais específicas ou URLs exclusivas.	Acessível apenas por redes criptografadas, como o Tor.
Conteúdo comum	Contém informações e sites disponíveis publicamente.	Inclui conteúdo não indexado por mecanismos de busca, como bancos de dados privados.	Contém conteúdo obscuro e frequentemente ilegal.
Anonimato	Não oferece anonimato especial para usuários.	Pode exigir credenciais de login, mas não	Valoriza altos níveis de anonimato e

		ênfatiza o anonimato.	segurança.
Conteúdo comercial	Amplamente usado para negócios, educação, entretenimento e informações públicas.	Inclui recursos protegidos por senha, como e-mails, serviços bancários online e redes corporativas.	Muitas vezes associada a atividades ilegais e conteúdo obscuro.
exemplos	Sites de notícias, blogs, redes sociais, sites de compras online.	E-mails privados, intranets corporativas, bancos de dados de bibliotecas.	Sites de venda de drogas, mercados negros, fóruns de hackers.

- **Surface Web (Web Superficial):** imagine a Internet como um iceberg no meio do oceano. A parte que você vê exposta acima da água é a Surface Web, que representa aquelas páginas acessíveis por mecanismos de busca convencionais, como o Google, Bing ou Yahoo. Essas páginas são públicas e facilmente encontradas, assim como a parte visível de um iceberg que está acima da água.
- **Deep Web (Web Profunda):** abaixo da superfície da água, onde o iceberg se estende, está a Deep Web. Nessa área, estão os conteúdos que não são indexados pelos motores de busca comuns, como páginas de bancos de dados, e-mails privados, áreas de login e muito mais. Você pode pensar na Deep Web como a parte do iceberg que está submersa, não visível à primeira vista, mas ainda acessível com as ferramentas certas, como senhas ou autorizações.
- **Dark Web (Web Escura):** agora, vá mais fundo nas águas escuras e misteriosas, onde a luz do sol não alcança. Lá você encontrará a Dark Web. Esta é a parte mais obscura e oculta da Internet, acessível por meio de redes criptografadas, como o Tor. A Dark Web é como a parte do iceberg que está profundamente submersa, invisível e intencionalmente oculta. É onde você pode encontrar sites que não querem ser rastreados e, às vezes, atividades ilegais.

1.12 Redes de Computadores - Parte 1 - Internet das Coisas - Teoria

Internet das Coisas (IoT)

INCIDÊNCIA EM PROVA: baixa

Vamos falar inicialmente sobre **Transformação Digital**. Para tal, vamos utilizar como referência um texto da Cisco Networking Academy:

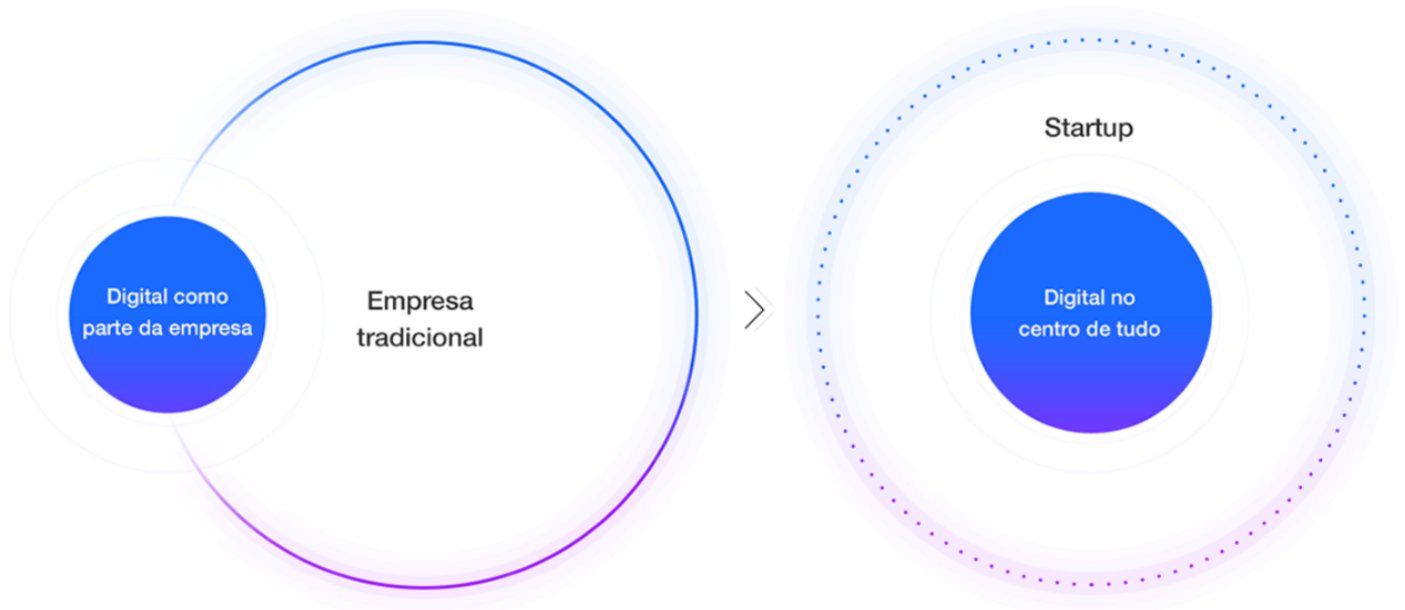
Diga a verdade ... quantos de vocês realmente poderiam passar o dia sem o smartphone?

No mundo de hoje, há mais dispositivos smart que pessoas. Um número cada vez maior de pessoas está conectado à Internet, de uma maneira ou de outra, 24 horas por dia. Um número crescente de pessoas possui e depende de três, quatro ou mais dispositivos smart. Esses dispositivos podem incluir smartphones, monitores de exercícios e saúde, leitores eletrônicos e tablets. Até 2020, prevê-se que cada consumidor terá em média 6,58 dispositivos smart. Como é possível que tantos dispositivos sejam conectados?

As redes digitais modernas tornam tudo isso possível. O mundo está sendo coberto rapidamente por redes que permitem a interconexão e a transmissão de dispositivos digitais. Pense na malha de redes como uma película digital ao redor do planeta. Com essa película digital, todos os dispositivos móveis, sensores eletrônicos, dispositivos de medição eletrônicos, dispositivos médicos e medidores podem se conectar. Eles monitoram, comunicam, avaliam e, em alguns casos, se adaptam automaticamente aos dados que estão sendo coletados e transmitidos.

À medida que a sociedade adota desses dispositivos digitais, as redes digitais continuam crescendo ao redor do mundo e os benefícios econômicos da digitalização continuam aumentando; podemos ver uma transformação digital. A transformação digital é a aplicação de tecnologia digital para fornecer o estágio para as empresas e a indústria inovarem. Agora esta inovação digital está sendo aplicada a todos os aspectos da sociedade humana.

Notem que a transformação digital pode ser definida como o **processo em que empresas usam tecnologias digitais inovadoras para integrar todas as áreas do negócio a fim de solucionar problemas, melhorar o desempenho, aumentar seu alcance e entregar valor ao cliente**. Trata-se de uma mudança estrutural/cultural nas organizações – e consequentemente na sociedade –, colocando a tecnologia com papel essencial para seu sucesso. Vejam a imagem a seguir:

Processo de transformação digital

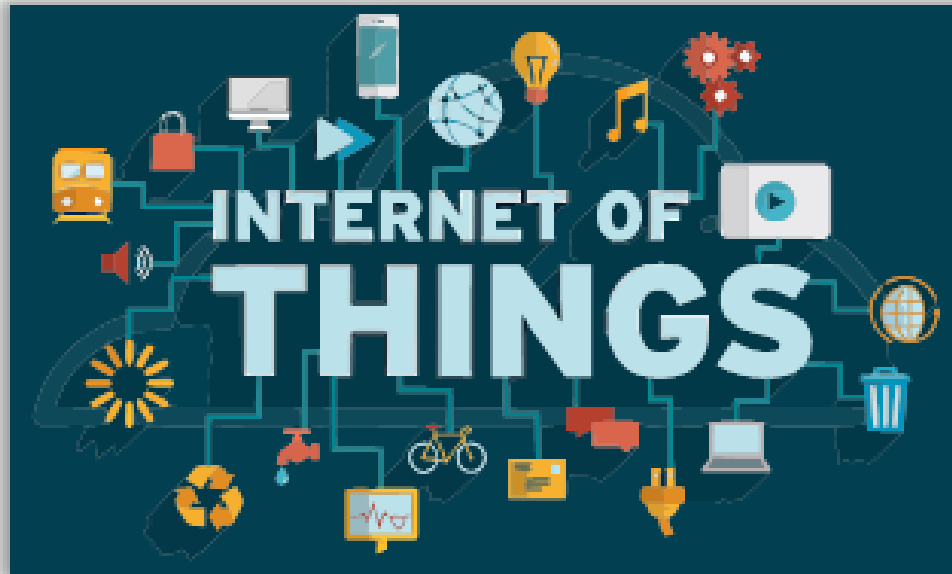
Galera, não há como fugir da transformação digital! *Querem um exemplo óbvio?* Eu estou desde o início da pandemia de coronavírus trabalhando remotamente. **O vírus basicamente acelerou de forma brutal o processo de transformação digital de órgãos e empresas – talvez, inclusive, de forma definitiva!** Em poucos dias, salas virtuais de reunião foram configuradas, acesso remoto foi concedido e novas formas de trabalho e avaliação surgiram. É a tecnologia no centro de tudo...

A retração econômica inicial por conta da COVID-19 obrigou empresas a fazerem difíceis cortes no orçamento. De forma simultânea, a pandemia impulsionou essas empresas a acelerarem seus esforços de transformação digital devido à demanda dos clientes, à limitação de interações pessoais e às necessidades dos funcionários em trabalho remoto. **Dito isso, vamos falar de uma tecnologia que vem para acelerar ainda mais o processo de transformação digital...**

INTERNET DAS COISAS

Trata-se de uma revolução tecnológica que se refere à conexão de dispositivos físicos e objetos do mundo real à internet. Esses dispositivos, também chamados de "coisas" na IoT, são integrados com sensores, software e outras tecnologias para coletar e trocar dados com outros dispositivos e sistemas pela internet.

Essa tecnologia que tem começado a cair em concurso público e que deve se popularizar com a chegada do 5G é a *Internet of Things (IoT)* – também conhecida como *Internet das Coisas*. Como é que é, professor? Galera, pensem rapidinho em todos os seus objetos que possuem acesso à internet: computador, notebook, *tablet*, smartphone, relógio, entre outros. Beleza, esses são os mais comuns em nosso dia a dia mesmo. Porém, vocês conseguem pensar em outros?



A câmera de segurança da portaria do seu prédio? **Ela tem acesso à internet!** A Smart TV que você assiste aquele filminho bacana na Netflix? **Ela tem acesso à internet!** Quem curte jogar um videogame de vez em quando? **Ele tem acesso à internet!** Galera, isso porque estamos no Brasil. Em outros países mais desenvolvidos, já existem outras coisas: geladeiras, máquina de lavar roupa, forno de micro-ondas, termostato, alarme de incêndio, sistema de som e iluminação, entre outros.

Isso não significa que seja possível baixar uma aula de informática no site do Estratégia Concursos usando sua geladeira! A proposta, na verdade, é que a conectividade auxiliará esses objetos a ficarem mais eficientes em seus contextos específicos. Agora vamos parar de

pensar na nossa casa e vamos pensar no mundo: isso tem aplicabilidades na agricultura, pecuária, hospitais, escolas, fábricas, transporte público, logística, etc.

contexto	descrição
Hospitalar	Pacientes podem utilizar dispositivos conectados que medem batimentos cardíacos ou pressão sanguínea, por exemplo, e os dados coletados serem enviados em tempo real para o sistema que controla os exames.
agricultura	Sensores espalhados em plantações podem dar informações precisas sobre temperatura, umidade do solo, probabilidade de chuvas, velocidade do vento e outras informações essenciais para o bom rendimento do plantio.
Pecuária	Sensores conectados aos animais conseguem ajudar no controle do gado: um chip colocado na orelha do boi pode fazer o rastreamento do animal, informar seu histórico de vacinas e assim por diante.
Indústria	Sensores podem medir, em tempo real, a produtividade de máquinas ou indicar quais setores da planta industrial precisam de mais equipamentos ou suprimentos.
Comércio	Prateleiras inteligentes podem informar, em tempo real, quando determinado item está começando a faltar, qual produto está tendo menos saída ou em quais horários determinados itens vendem mais.
Transporte	Usuários podem saber, pelo smartphone ou em telas instaladas nos pontos, qual a localização de determinado ônibus. Os sensores também podem ajudar a empresa a descobrir que um veículo apresenta defeitos mecânicos, assim como saber como está o cumprimento de horários.
Logística	Dados de sensores instalados em caminhões, contêineres e até caixas individuais combinados com informações do trânsito podem ajudar a definir melhores rotas, escolher veículos mais adequados para determinada área, quais encomendas distribuir entre a frota ativa, etc.

IoT não é uma tecnologia monolítica. Logo, seus componentes principais podem variar bastante, mas – em regra – incluem:

Componentes	descrição
-------------	-----------

Dispositivos	São os elementos físicos que compõem a IoT, como sensores, atuadores e outros dispositivos conectados, como câmeras, medidores inteligentes, veículos e eletrodomésticos. Eles coletam dados do mundo real e podem executar ações com base nesses dados.
Tecnologias de comunicação	São os meios pelos quais os dispositivos IoT se comunicam entre si e com a nuvem. Isso pode incluir Wi-Fi, Bluetooth, 3G/4G/5G, Zigbee, LoRa, entre outros. As redes de comunicação são responsáveis pela transferência de dados dos dispositivos para a nuvem e vice-versa.
Sensores e Atuadores	Os sensores coletam informações do ambiente, como temperatura, umidade, localização, movimento e muito mais. Os atuadores são responsáveis por tomar ações, como ligar ou desligar um dispositivo. Eles são os olhos e as mãos da IoT.
Nuvem (cloud)	A nuvem é onde os dados coletados pelos dispositivos IoT são processados, armazenados e disponibilizados para acesso. Plataformas de nuvem fornecem recursos de computação, armazenamento e análise de dados em grande escala, tornando possível o processamento de grandes volumes de informações.

Imagine uma casa que tem monitoramento de segurança, controle de temperatura ambiente e gerenciamento de iluminação integrados. Os dados de câmeras, alarmes contra incêndio, aparelhos de ar-condicionado, lâmpadas e outros itens são enviados para um sistema que controla cada aspecto. **Esse sistema pode ser um serviço em nuvem, garantindo acesso a ele a partir de qualquer lugar.**

Lembrando que o IPv6 (evolução do IPv4) permitiu a oferta de um número absurdamente gigantesco de endereços, logo a quantidade de dispositivos e sensores não deverá ser um problema por um bom tempo. É importante destacar também que a comunicação é um elemento essencial para a transmissão de dados entre dispositivos, sensores e sistemas de IoT. Abaixo, veremos algumas das principais tecnologias e protocolos de comunicação utilizados na IoT:

Tecnologias de comunicação	descrição
-----------------------------------	------------------

Wi-fi (802.11)	Trata-se de uma das tecnologias de comunicação sem fio mais amplamente utilizadas e oferece alta largura de banda. É adequado para dispositivos que têm acesso a redes locais de alta velocidade e energia suficiente.
Bluetooth (802.15)	Trata-se de uma tecnologia de comunicação sem fio de curto alcance, adequada para dispositivos pessoais, como fones de ouvido sem fio e dispositivos vestíveis. O Bluetooth Low Energy (BLE) é uma variante de baixo consumo de energia.
Zigbee	Trata-se de um padrão de comunicação sem fio de baixa potência projetado para redes de sensores e dispositivos IoT em ambientes domésticos e industriais.
Lora (long range)	Trata-se de uma tecnologia de comunicação de longo alcance e baixa potência usada em aplicações de IoT em áreas remotas. É ideal para sensores que precisam de comunicação em longas distâncias.
Sigfox	Trata-se de uma rede de baixa potência e baixa largura de banda projetada para aplicações de IoT que enviam pequenas quantidades de dados.
Nb-iot	Trata-se de um padrão de comunicação de baixa potência baseado em redes celulares para dispositivos IoT que exigem baixo consumo de energia e cobertura ampla.

Poxa, Diego... IoT só tem coisas boas! Calma, não é bem assim! **Os dispositivos podem eventualmente estar vulneráveis a ataques de segurança e privacidade.** Existe uma infinidade de riscos associados à IoT, tais como: riscos de um dispositivo permitir o acesso não autorizado e o uso indevido de informações pessoais; riscos de facilitar ataques em outros sistemas, escalonando privilégios ao invasor; riscos de os dispositivos servirem de escravos em botnets; entre outros.

Vantagens	desvantagens
Varejistas podem fornecer bônus de fidelidade para clientes preferenciais.	A dependência de compras online pode custar empregos.

As cidades podem avaliar as necessidades futuras de transporte.	Os varejistas podem saber tudo o que você está comprando.
Indivíduos podem reduzir os custos de energia e dos sistemas de aquecimento residenciais.	Os indivíduos podem receber mais e-mails de spam.
Fabricantes podem reduzir a inatividade prevendo as necessidades de manutenção dos equipamentos.	Uma falha da rede pode ser catastrófica.
Os governos podem monitorar o ambiente.	As empresas que criam dispositivos vestíveis têm muitas informações pessoais sobre os usuários.

É importante mencionar que a IoT – em geral – utiliza uma tecnologia chamada Long-Range Low-Power Wide Area Network, isto é, um tipo de rede sem fio de longa distância que permite comunicações com baixa taxa de transmissão de dados e baixo consumo de energia. A ideia do IoT é transmitir dados a grandes distâncias e, inclusive, a partir de dispositivos à bateria. **Apenas para comparação, o Bluetooth é uma tecnologia Short-Range Low-Power Personal Area Network.**

Finalmente, a IoT poderia ser definida, portanto, como uma tecnologia que permite que uma malha de dispositivos – **tais como dispositivos móveis, wearables (tecnologias para vestir), sensores, aparelhos eletrônicos de consumo e domésticos, dispositivos automotivos e dispositivos ambientais**– possam ser integrados para acessar aplicativos e informações ou para a interação com pessoas, redes sociais, governos e empresas.

1.13 Redes de Computadores - Parte 1 - Tecnologias de Acesso - Teoria

Tecnologias de Acesso

TECNOLOGIAS DE ACESSO À INTERNET

Referem-se aos métodos e infraestruturas utilizados para conectar dispositivos, como computadores, smartphones e outros equipamentos, à Internet. Essas tecnologias permitem que os dispositivos acessem os serviços e recursos disponíveis na World Wide Web e em

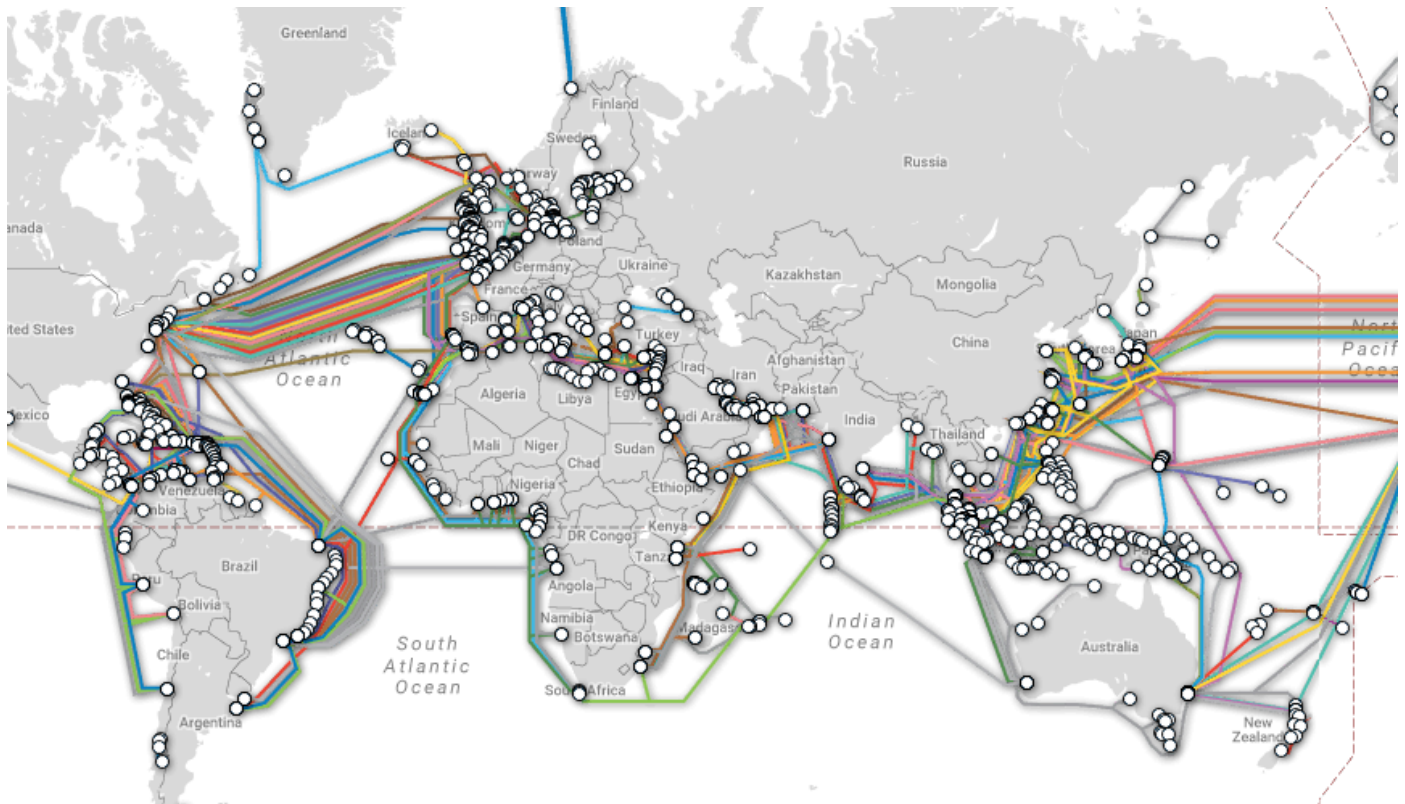
outros serviços online. Existem várias tecnologias de acesso à Internet (Ex: Dial-Up, ADSL, HFC, Fibra Óptica, PLC, Radiodifusão, Satélite e Telefonia Móvel), e a escolha depende das necessidades e da disponibilidade em uma determinada região.

Galera, até o início da década de noventa, só quem sabia o que era internet eram pesquisadores ligados a universidades, ao governo ou à indústria. No entanto, quando um físico chamado Tim Berners-Lee criou a Web (WWW), houve uma mudança nessa realidade e a internet ganhou milhões de novos usuários sem a menor pretensão acadêmica. **O serviço de disponibilização de páginas web facilitou e popularizou bastante o uso da internet.**

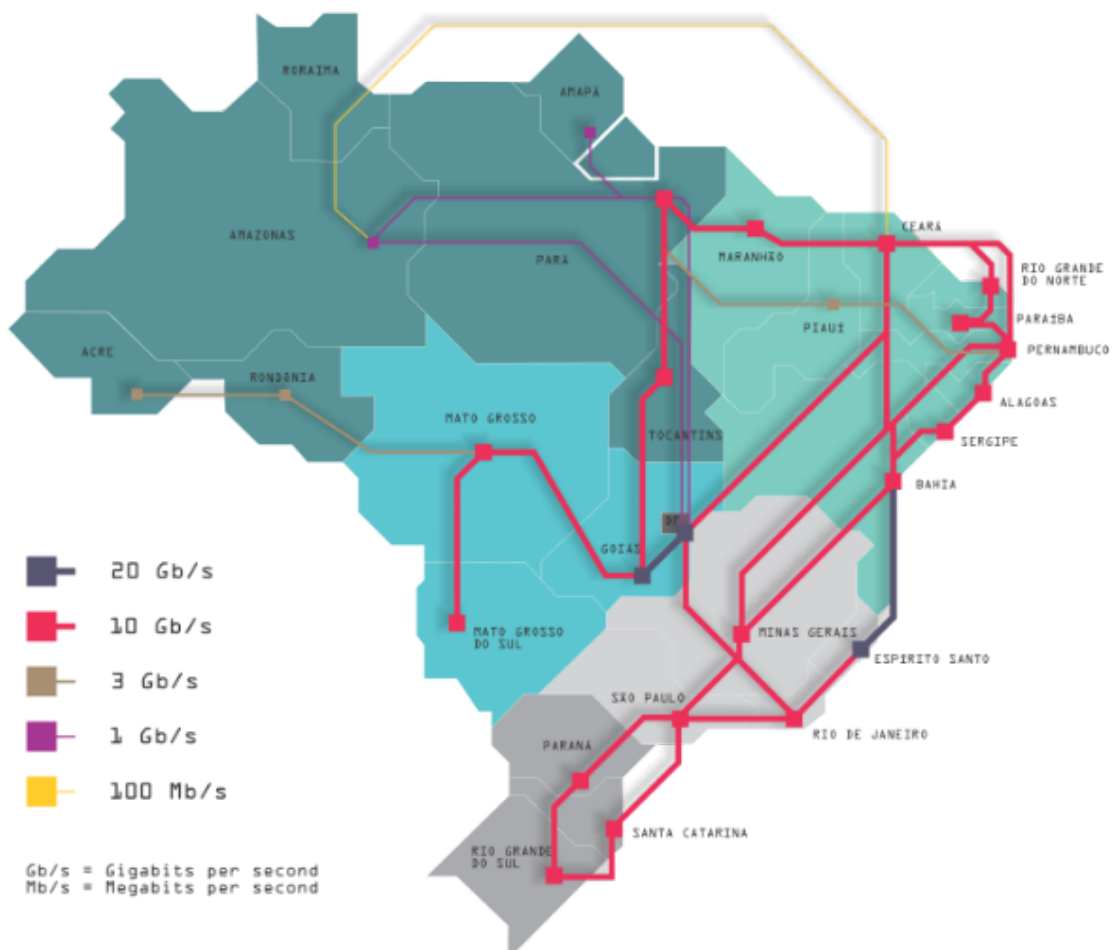
Junto com o primeiro navegador da história (chamado Mosaic), a web tornou possível a configuração de diversas páginas web contendo informações, textos, imagens, sons e vídeos disponíveis através de links para outras páginas. Clicando em um link, o usuário é repentinamente transportado para a página indicada por esse link. **Com o passar dos anos, foram criadas muitas páginas em um período de tempo muito curto.**

Grande parte desse crescimento foi impulsionado por empresas denominadas Provedores de Serviços da Internet (ISP – Internet Service Provider). Essas empresas oferecem a usuários individuais a possibilidade de se conectar à Internet, obtendo assim acesso aos diversos serviços fornecidos. Essas empresas reuniram milhões de novos usuários, alterando completamente o perfil de usuário sendo utilizada como um serviço de utilidade pública (como a telefonia).

Vamos detalhar isso melhor! A internet pode ser fornecida por meio de satélites, ondas de rádio ou uma rede de milhares de cabos de fibra óptica terrestres ou submarinos, que conectam diversos países, respondendo por 80% de toda a comunicação. **Essa infraestrutura de redes – que forma a espinha dorsal da internet – é chamada de Backbone. Ela possui alto velocidade, desempenho e interliga várias redes, garantindo o fluxo da informação por dimensões continentais.**



National Research Network BACKBONE



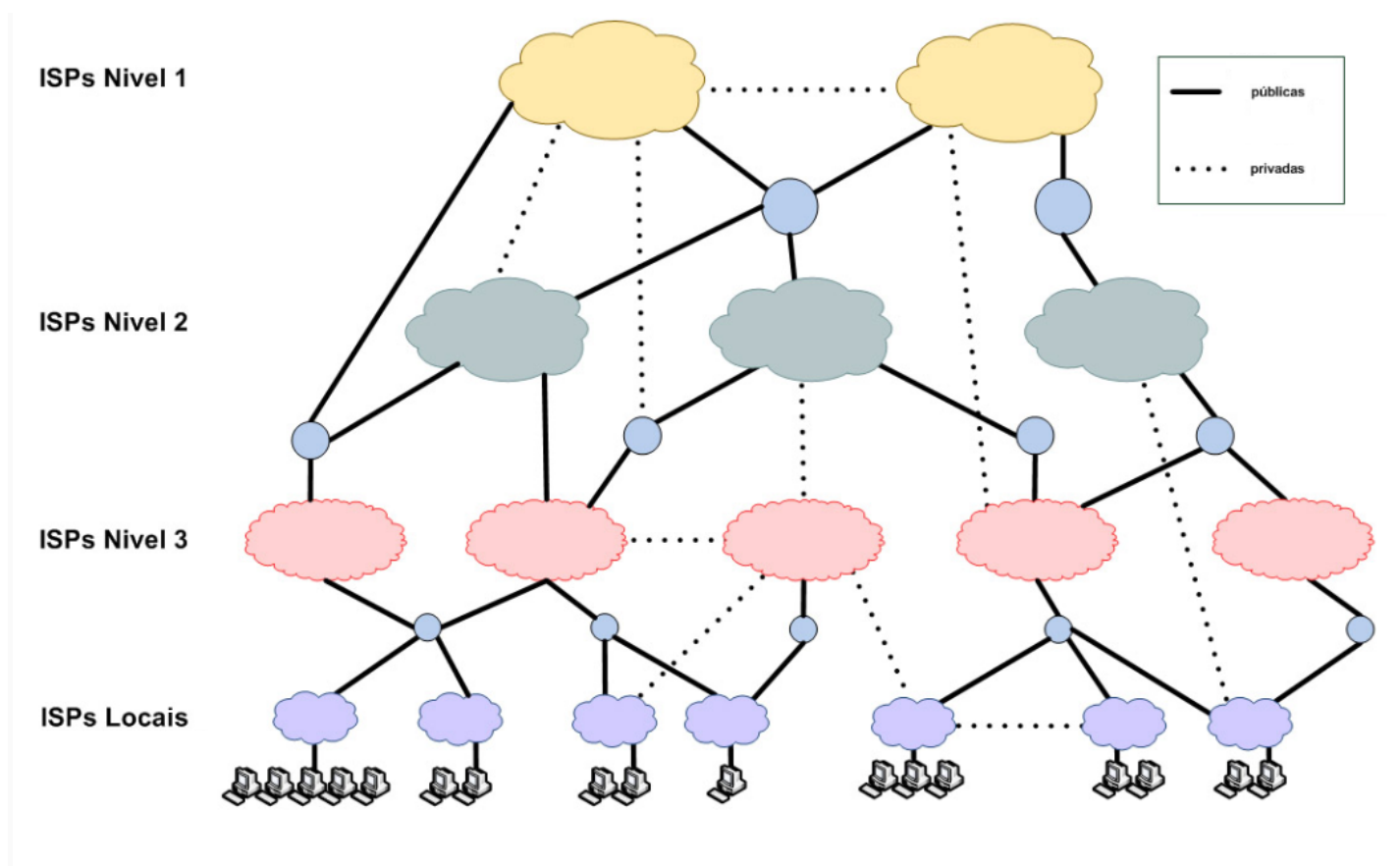
Diego, quem constrói esses backbones? Eles são construídos por provedores de serviço de internet, que administram troncos de longo alcance com o objetivo de fornecer acesso à internet para diversas outras redes. Em geral, eles pertencem a companhias telefônicas de longa distância (Ex: Embratel) ou a governos nacionais (Ex: Rede Nacional de Ensino e Pesquisa – RNP), **que vendem o acesso para Provedores de Serviço de Internet (ISP – Internet Service Provider).**

Os provedores de internet nacionais mais conhecidos atualmente são: NET/CLARO, GVT/VIVO e SKY. Por sua vez, esses provedores de internet vendem o acesso a provedores menores ou a usuários comuns. Na imagem anterior, é possível visualizar os maiores troncos de backbones espalhados pelo mundo entre os continentes e também os troncos de backbones brasileiros. Notem que eles podem ser terrestres ou submarinos. Existem três níveis de provedores de acesso:

Níveis	Descrição
ISP nível 1	São os provedores de acesso à internet de nível mais alto na hierarquia. Eles não precisam comprar acesso à internet de outros provedores, pois possuem uma rede global de alta capacidade e trocam tráfego diretamente uns com os outros. Exemplos de provedores de Nível 1 incluem AT&T, Verizon, NTT Communications e CenturyLink. Eles têm uma presença global e fornecem acesso à internet em escala internacional. Imagine ISPs de Nível 1 como rodovias federais, como a Rodovia Presidente Dutra (BR-116). Essas rodovias cruzam continentes e países sem precisar pagar pedágio a outras estradas menores. Os provedores de Nível 1 constroem e mantêm essas "rodovias da internet" e interconectam-se diretamente para permitir um tráfego rápido e eficiente.
ISP nível 2	Estes são provedores de acesso à internet que não possuem redes globais como os Nível 1, mas ainda têm uma rede significativa em uma área geográfica específica. Eles geralmente compram acesso à internet de Nível 1 ISPs e podem vender serviços a ISPs de nível inferior ou a empresas e consumidores diretos. Exemplos de provedores de Nível 2 incluem Cogent, Orange, Charter, Deutsche Telekom, entre outros.

	ISPs de Nível 2 podem ser comparados a rodovias estaduais. Eles atendem a áreas geográficas maiores, como estados ou regiões inteiras. Essas rodovias estaduais se conectam às autoestradas globais (Nível 1) e podem cobrar pedágio por permitir que o tráfego flua entre essas grandes autoestradas e áreas locais.
ISP nível 3	São provedores regionais ou locais que não possuem redes globais. Eles compram acesso à internet de provedores de Nível 1 ou 2 para fornecer conectividade a empresas e consumidores em áreas geográficas específicas. Esses ISPs podem se concentrar em uma única cidade, região ou país. Alguns provedores de Nível 3 podem ser ISPs de acesso final, que fornecem serviços diretamente a residências e empresas locais. ISPs de Nível 3 são como as estradas locais e ruas em cidades. Eles atendem áreas geográficas muito específicas, como uma cidade ou bairro. Essas estradas locais se conectam às rodovias regionais (Nível 2) ou diretamente às autoestradas globais (Nível 1) e permitem que o tráfego alcance destinos locais.

ISPs Locais normalmente se enquadram como ISPs de Nível 3. Eles são responsáveis por fornecer conectividade à Internet para áreas locais específicas e são mais próximos dos usuários finais.



Dito isso, os enlaces que conectam as redes de acesso residenciais aos ISP Nível 3 ou Locais podem ser de diferentes tecnologias, vamos conhecê-las a seguir:

Tecnologias de acesso	Descrição
Dial-up	Uma tecnologia de acesso discado à internet que utiliza a linha telefônica tradicional. É lenta e está em desuso na maioria das áreas.
Adsl	Uma tecnologia de acesso de banda larga que utiliza a linha telefônica para fornecer velocidades mais rápidas do que o dial-up.
Hfc	Uma tecnologia que combina fibra óptica e cabos coaxiais para fornecer serviços de internet de alta velocidade e TV a cabo.
Fibra óptica	Uma tecnologia de alta velocidade que utiliza cabos de fibra óptica para transmitir dados em alta velocidade por meio de pulsos de luz.
Plc	Utiliza a rede elétrica para transmitir dados, tornando a fiação elétrica existente uma rede de comunicação.

Radiodifusão	Utiliza ondas de rádio para transmitir dados. Pode incluir tecnologias como Wi-Fi e redes celulares.
Satélite	Acesso à internet via satélite – os dados são enviados e recebidos por meio de satélites em órbita terrestre.
Telefonia móvel	Acesso à internet usando redes móveis (3G, 4G, 5G), permitindo a conexão em movimento a partir de dispositivos móveis.

Dial-Up

INCIDÊNCIA EM PROVA: média

Trata-se de uma conexão discada através de um modem e uma linha de telefonia fixa. Era a maneira mais popular de acesso da década de 90, hoje encontra-se em desuso. Apresenta um alto custo de implementação, é bastante instável e possui baixas taxas de transmissão. *Era banda larga?* Não, era banda estreita – com taxas máximas de 56Kbps. Se hoje você reclama que a sua internet de 100 Mbps está lenta, lembre-se que uma internet discada era 2000x mais lenta!

dial-up	Descrição
Conexão por linha	A conexão Dial-Up utiliza a linha telefônica convencional para estabelecer a conexão com a Internet. Isso significa que o acesso à Internet é estabelecido por meio de uma chamada telefônica.
Baixa velocidade	Uma das principais desvantagens da conexão Dial-Up é a baixa velocidade de transmissão de dados. As velocidades típicas variam de 56 kbps a 128 kbps, o que é significativamente mais lento do que tecnologias mais recentes.
Conexão discada	Os usuários precisam discar para o Provedor de Serviços de Internet (ISP) toda vez que desejam se conectar à web. Isso envolve o uso de um modem Dial-Up para criar a conexão, o que pode levar um tempo considerável.
Linha ocupada	Uma das desvantagens mais notáveis é que, enquanto você está conectado via Dial-Up, a linha telefônica fica ocupada. Isso significa

	que você não pode fazer ou receber chamadas telefônicas ao mesmo tempo em que está conectado à Internet.
Custos de chamada telefônica	A conexão Dial-Up requer uma chamada telefônica para o ISP. Dependendo do plano telefônico, isso pode resultar em custos adicionais. Em alguns lugares, as chamadas telefônicas locais eram gratuitas, enquanto em outros lugares eram tarifadas.
Desconexões frequentes	A conexão Dial-Up é vulnerável a quedas frequentes devido a interferências na linha telefônica ou outras questões técnicas. Isso pode ser frustrante para os usuários, pois eles precisam se reconectar repetidamente.
Incompatibilidade com conteúdo rico	Devido à baixa velocidade, a conexão Dial-Up não é adequada para acessar conteúdo rico em multimídia, como vídeos de alta qualidade ou jogos online. O streaming de mídia pode ser lento e de baixa qualidade.
Obsoleta	A tecnologia Dial-Up é considerada obsoleta na maioria das regiões do mundo, com provedores de serviços migrando para tecnologias de banda larga mais rápidas, como DSL, cabo, fibra óptica e redes móveis 3G/4G/5G.
Baixa largura de banda	A largura de banda limitada da conexão Dial-Up torna o uso de aplicativos intensivos em largura de banda, como videoconferências ou transferências de arquivos grandes, uma tarefa lenta e complicada.
Adequada para tarefas básicas	Embora seja inadequada para muitas atividades online modernas, a conexão Dial-Up ainda pode ser adequada para tarefas básicas, como envio e recebimento de e-mails, navegação na web com páginas leves e chat online.

ADSL

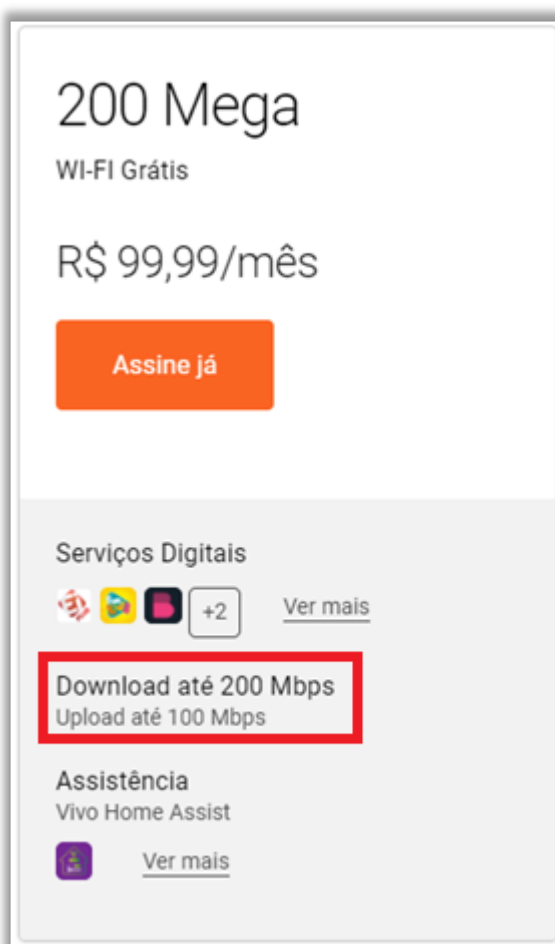
INCIDÊNCIA EM PROVA: média

Trata-se da conexão de banda larga (assim como todas as outras que veremos a seguir) oferecida por empresas de telefonia fixa. ADSL é a sigla para *Asymmetric Digital Subscriber Line* ou Linha de Assinante Digital Assimétrica. Essa tecnologia possui uma grande vantagem: embora utilize a mesma infraestrutura da telefonia, a transmissão de dados ocorre em frequências mais altas que as de voz, permitindo – portanto – o uso da internet sem ocupar o

telefone.

Professor, por que essa é uma tecnologia assimétrica? **Porque as taxas de download e de upload são diferentes – sendo a velocidade de download maior que a de upload.** Vocês sabiam disso? Quando nós contratamos um serviço de internet via ADSL, nós sempre olhamos a taxa de download e esquecemos a taxa de upload. Na minha casa, eu assinei um serviço de 100mbps! Notem que essa é a taxa (máxima) de download – a taxa de upload é bem menor.

Vejam no exemplo seguinte que a taxa de download à esquerda é de 200 mbps e a taxa de upload é de 100 mbps; a taxa de download à direita é de 200 mbps e a taxa de upload é 60 mbps. *Isso faz diferença, Diego?* Dependerá do seu perfil de utilização! **Se você costuma apenas fazer navegar na web, assistir um filme, baixar aulas – não há nenhum problema; mas se você tem um canal no Youtube e precisa fazer uploads de vídeos grandes – pode ser inconveniente.**



200 Mega

Wi-Fi Grátis

R\$ 99,99/mês

[Assine já](#)

Serviços Digitais

 +2 [Ver mais](#)

Download até 200 Mbps
Upload até 100 Mbps

Assistência

Vivo Home Assist

 [Ver mais](#)

200 Mega

Ideal para 7 a 10 dispositivos

Você e sua família podem ver vídeos e filmes em 4K, jogar online e fazer downloads. Tudo ao mesmo tempo.

De R\$119,90

R\$ 99,90

/MÊS

No Débito em Conta e Conta Digital.

CONSULTAR DISPONIBILIDADE

Informações da oferta:

- ✓ Fixo Ilimitado
- ✓ Modem WiFi UP
- ✓ Instalação grátis
- ✓ 60 Mega de upload

adsl	Descrição
Assimétrica	O "A" em ADSL significa assimétrico, o que indica que a taxa de upload (envio de dados) é diferente da taxa de download (recebimento de dados). Geralmente, a taxa de download é significativamente mais rápida do que a de upload.
Utilização das linhas telefônicas	O ADSL utiliza as linhas telefônicas convencionais para transmitir dados. Ele é compatível com a infraestrutura de telefone existente, permitindo que os usuários acessem a Internet e façam chamadas telefônicas simultaneamente.
Frequências diferentes	Linhas telefônicas transmitem dados em diferentes frequências. As frequências mais baixas são reservadas para voz, enquanto as frequências mais altas são usadas para transmitir dados. Isso permite que a Internet e as chamadas coexistam na mesma linha.
Velocidade variável	A velocidade da conexão ADSL pode variar de acordo com a distância entre o usuário e a central telefônica. Quanto mais longa a linha

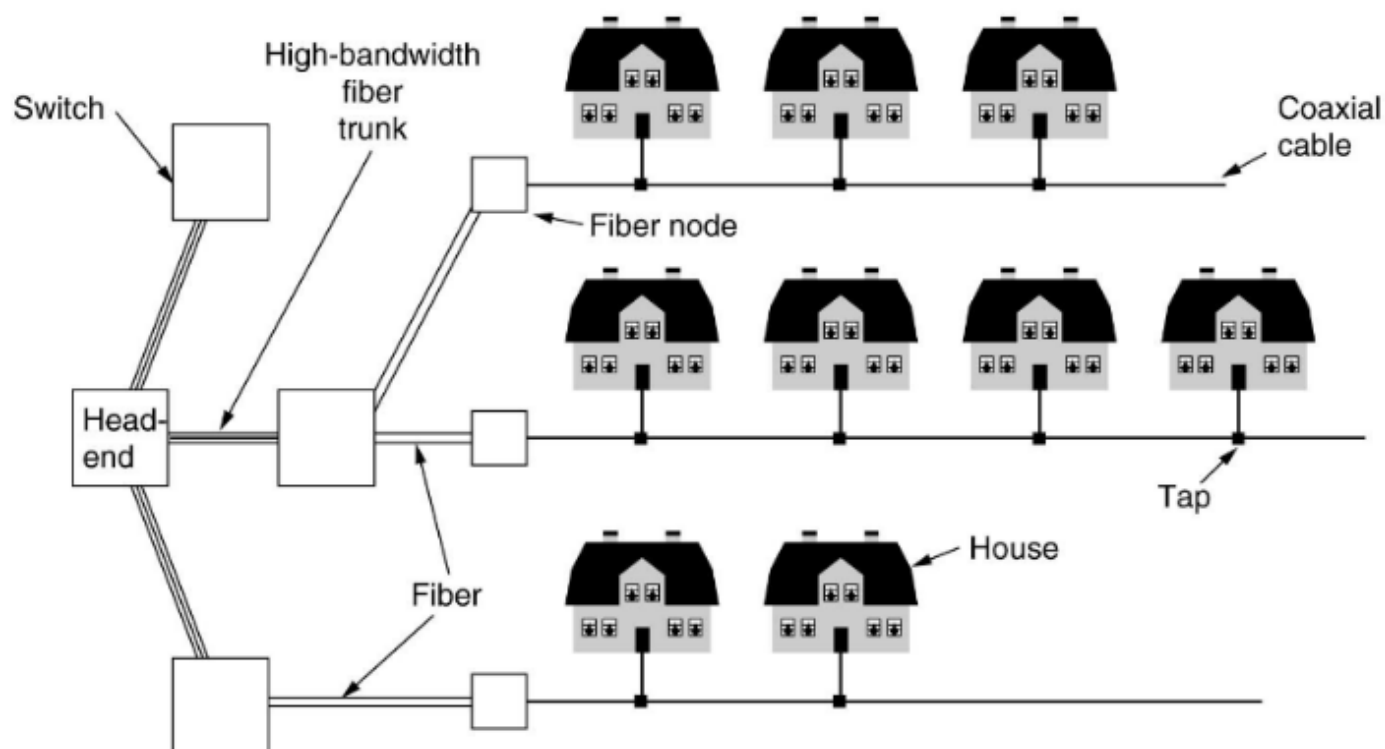
	telefônica, mais lenta é a conexão. Isso ocorre porque o sinal ADSL enfraquece à medida que viaja por distâncias maiores.
Taxa de upload limitada	A taxa de upload no ADSL é geralmente menor do que a de download. Isso significa que o envio de dados, como o carregamento de arquivos ou o envio de e-mails com anexos grandes, é mais lento do que o download.
Largura de banda compartilhada	A largura de banda em uma linha ADSL é compartilhada entre todos os usuários conectados a essa linha. Isso significa que, em horários de pico, a velocidade da conexão pode diminuir devido à concorrência por largura de banda.
Adequada para aplicações residenciais	O ADSL é frequentemente usado em ambientes residenciais. É adequado para atividades como navegação na web, streaming de vídeos em qualidade padrão e jogos online.
Ampla disponibilidade	Devido à utilização das linhas telefônicas existentes, o ADSL é amplamente disponível em muitas áreas urbanas e rurais. No entanto, a velocidade da conexão pode variar dependendo da localização geográfica.
Requer um modem adsl	Os usuários precisam de um modem ADSL para estabelecer a conexão. Esse modem é fornecido pelo provedor de serviços de Internet ou pode ser adquirido separadamente.
Superado por tecnologias mais rápidas	Embora ainda seja utilizado, o ADSL foi superado por tecnologias de banda larga mais rápidas, como a fibra óptica e o cabo, que oferecem velocidades mais altas e uma experiência de Internet mais fluida.

HFC

INCIDÊNCIA EM PROVA: baixíssima

Trata-se da conexão híbrida de banda larga via cabos de concessionárias de TV a Cabo (NET, GVT, OI). HFC é a sigla para *Hybrid Fiber-Coax* e representa o hibridismo entre fibra óptica e cabo coaxial. *Por que é um hibridismo, Diego?* Porque os cabos de fibra óptica partem do backbone central, passam pelos postes até chegar mais próximo das residências e se

conectar a um receptor óptico. A partir daí, cabos coaxiais saem do receptor e distribuem o sinal entre as casas.



É interessante mencionar que esses cabos coaxiais que saem do receptor para distribuir o sinal entre as casas funciona como um barramento compartilhado, logo com transmissão em broadcast. HFC e ASDSL são tecnologias concorrentes: ambas são assimétricas e possuem taxas de transmissão semelhantes, porém a primeira é fornecida por empresas de TV a Cabo e a segunda é oferecida por empresas de telefonia fixa.

hfc	Descrição
Híbrida	A sigla HFC significa "Híbrido de Fibra-Coaxial". Essa tecnologia combina o uso de cabos de fibra óptica e cabos coaxiais para a transmissão de dados. A fibra óptica é utilizada na infraestrutura principal, enquanto os cabos coaxiais são usados para a distribuição local.
Canais separados	No HFC, os dados são transmitidos em canais separados. Isso permite a transmissão simultânea de vários serviços, como Internet, TV a cabo e voz sobre IP (VoIP), sem interferência.
Velocidade de download e upload	O HFC geralmente oferece uma largura de banda significativa, permitindo altas velocidades de download e upload. Isso é adequado para atividades que requerem largura de banda, como streaming de vídeo em alta definição e jogos online.
Baixa latência	A tecnologia HFC tende a ter baixa latência, o que a torna adequada para aplicações em tempo real, como chamadas de vídeo e jogos online.

Adequado p/ redes de tv a cabo	Além do acesso à Internet, o HFC é frequentemente usado para fornecer serviços de televisão a cabo. Os provedores de TV a cabo aproveitam a alta capacidade da fibra óptica para transmitir uma grande variedade de canais de TV.
Modens e roteadores específicos	Os usuários de HFC precisam de modems e roteadores específicos para se conectarem à Internet. Esses dispositivos são fornecidos pelos provedores de serviços ou podem ser adquiridos separadamente.
Ampla disponibilidade urbana	A tecnologia HFC é amplamente disponível em áreas urbanas e suburbanas, onde a infraestrutura de cabo coaxial já está estabelecida.
Oferece pacotes de serviços	Os provedores de serviços de HFC geralmente oferecem pacotes que incluem acesso à Internet, TV a cabo e serviços de voz. Isso permite que os usuários escolham o que desejam com base em suas necessidades.
Concorrência no mercado	Em muitas áreas, o HFC enfrenta concorrência de outras tecnologias de acesso à Internet, como fibra óptica, DSL e conexões sem fio. Isso muitas vezes leva a preços competitivos e opções variadas para os consumidores.

#VamosPraticar#

(PROF. DIEGO / INÉDITA – 2023) HFC é uma tecnologia que utiliza tanto fibra óptica quanto cabos coaxiais para fornecer serviços de internet e TV a cabo.

Comentários: na verdade, as redes HFC têm uma parte inicial de fibra óptica, que é usada para transmitir dados a longas distâncias, e uma parte final de cabos coaxiais, que levam os dados diretamente para as casas dos assinantes. É uma solução híbrida que combina as vantagens de ambas as tecnologias (Correto).

#VamosPraticar#

Fibra Óptica

INCIDÊNCIA EM PROVA: baixíssima

Muito mais internet num único plano.

VIVO TOTAL*

FIBRA 300 MEGA + CELULAR 50 GIGA Por R\$ 189,99/mês

📞 Curtiu? Fale com a gente.
vivo.com.br | Consulte condições.

Destrave seu home office com ultravelocidade.

VIVO FIBRA

Oferta exclusiva até 30/07

200 MEGA R\$ 99,99/mês

📞 Quer saber mais? Fale com a gente.
3831-2525 | 9 9922-1614 | 3831-7090
vivo.com.br/vivofibra

sujeito a análise de crédito e concessão de fidelidade de 12 meses. Consulte condições gerais.

Trata-se da conexão direta via fibra óptica até a residência do contratante do serviço de internet. Pois é, já existe tecnologia que permite uma conexão direta até a sua casa por meio de um cabo de fibra óptica. Ainda não está disponível em diversas localizações (como a minha casa), mas essa tecnologia tende a se popularizar. *Você já tem na sua região?* Vamos ver agora as suas principais características:

Fibra óptica	Descrição
Alta velocidade	A principal característica da fibra óptica é a alta velocidade de transmissão de dados. A luz é usada para transmitir informações através das fibras, o que permite taxas de transferência de dados extremamente rápidas.
Alta Largura de banda	A fibra óptica oferece uma largura de banda significativa, tornando-a adequada para lidar com grandes volumes de dados, incluindo streaming de vídeo em alta definição, videoconferências, jogos online e transferências de arquivos pesados.
Baixa atenuação	A luz viaja por longas distâncias na fibra óptica com pouca perda de sinal, resultando em alta qualidade e consistência na transmissão de dados.

Imunidade a interferência	As fibras ópticas não são suscetíveis a interferências eletromagnéticas, o que significa que não são afetadas por campos elétricos ou magnéticos.
Segurança de dados	Como os sinais são transmitidos como luz, é difícil interceptar ou invadir uma conexão de fibra óptica, tornando-a uma opção segura para a transmissão de dados sensíveis.
Distâncias longas	A fibra óptica pode transmitir dados a distâncias muito maiores do que outros meios de transmissão, sem perda significativa de sinal.
Baixa latência	A baixa latência é uma característica da fibra óptica, o que a torna ideal para aplicações que exigem respostas rápidas, como jogos online e videoconferências.
Variedade de serviços	A fibra óptica é usada para fornecer serviços de Internet de alta velocidade, televisão digital, telefonia VoIP e muito mais.
Leveza e dimensões reduzidas	Os cabos de fibra óptica são leves e têm um tamanho compacto em comparação com cabos de cobre, tornando a instalação mais fácil e econômica.
Menos suscetibilidades a intempéries	Os cabos de fibra óptica são menos suscetíveis a danos causados por condições climáticas adversas, como tempestades e raios.
Infraestrutura de próxima geração	A fibra óptica é considerada uma tecnologia de acesso que atende às demandas das futuras redes de alta velocidade e é um componente importante para o desenvolvimento de infraestruturas de comunicação de próxima geração.

Crescente disponibilidade	Embora ainda não esteja disponível em todas as áreas, a disponibilidade de redes de fibra óptica está aumentando, especialmente em áreas urbanas.
Maior preço	A fibra óptica tende a ser mais cara de implementar em comparação com outras tecnologias de acesso, devido aos custos de infraestrutura.
Manutenção complexa	Embora a fibra óptica seja durável, a manutenção pode ser mais complexa e cara quando comparada a outros meios de transmissão.
Necessidade de conversores	Para uso em dispositivos convencionais, é necessário o uso de conversores para transformar os sinais ópticos em sinais elétricos.

#VamosPraticar#

(PROF. DIEGO / INÉDITA – 2023) A fibra óptica é uma tecnologia de acesso à internet que possui maior latência em comparação com conexões de cabo.

Comentários: a fibra óptica é conhecida por ter menor latência em comparação com muitas outras tecnologias de acesso à internet, tornando essa afirmação falsa (Errado).

#VamosPraticar#

PLC

INCIDÊNCIA EM PROVA: baixíssima

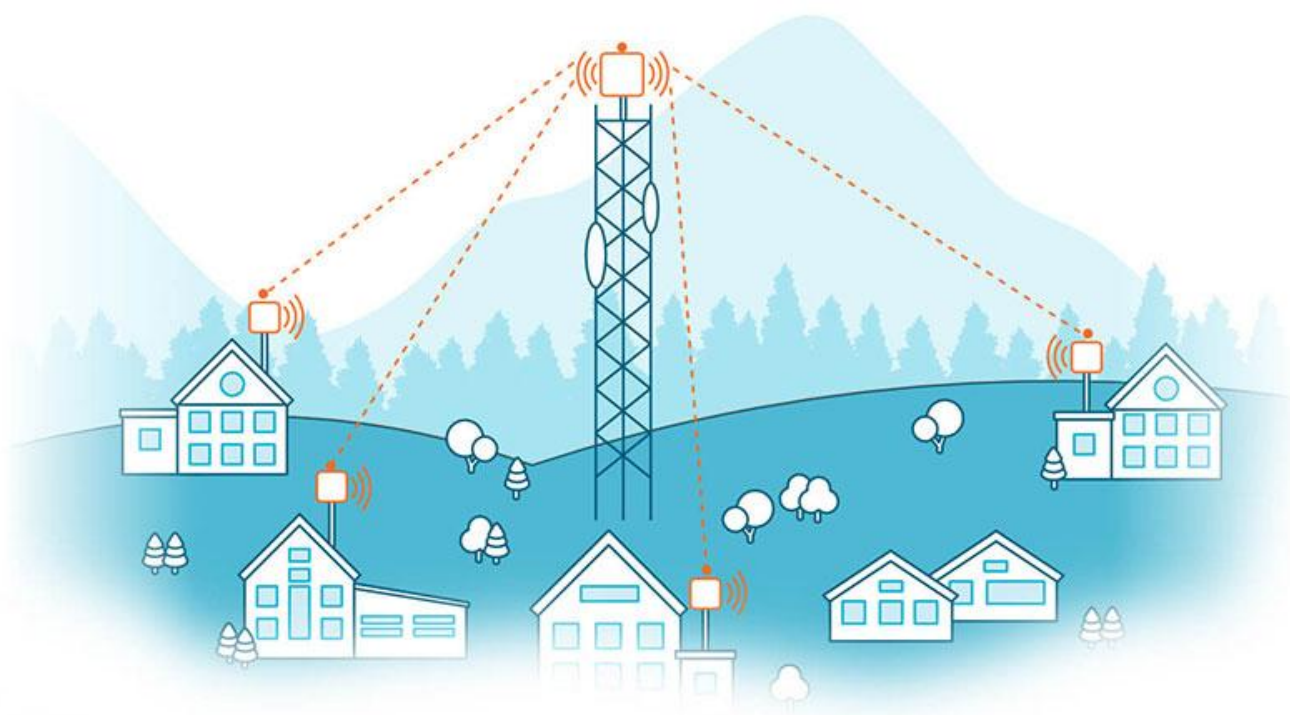
Trata-se da tecnologia que permite o acesso à internet banda larga via rede elétrica. PLC é a sigla para *Power Line Communication*. Como assim, professor? Como vantagem, é uma tecnologia bastante portátil, visto que basta plugar o modem em uma tomada compatível com o serviço para se obter o acesso. No Brasil, embora o serviço seja autorizado pelas agências responsáveis, os investimentos foram baixos por questões estratégicas e econômicas.

plc	Descrição
Uso de Infraestrutura elétrica	O PLC utiliza a rede elétrica preexistente para transmitir dados. Isso significa que não são necessários cabos de rede adicionais, como os usados em conexões Ethernet tradicionais.
Facilidade de instalação	A instalação é relativamente simples. Em geral, usuários precisam de um adaptador PLC que é conectado a uma tomada elétrica e ao roteador. Outros adaptadores podem ser conectados a tomadas em diferentes partes da residência para estender a cobertura.
Velocidade variável	A velocidade da conexão pode variar dependendo de vários fatores, incluindo a qualidade da fiação elétrica e a distância entre os adaptadores. Em comparação com outras tecnologias, como fibra óptica ou DSL, o PLC tende a oferecer velocidades mais baixas.
Alcance limitado	A eficácia do PLC pode diminuir à medida que a distância entre os adaptadores aumenta. Isso pode limitar a sua utilidade em residências maiores ou edifícios com fiação elétrica mais antiga.
Conexão estável	Em condições ideais, a conexão PLC pode ser bastante estável. No entanto, a presença de ruídos na rede elétrica ou dispositivos elétricos que geram interferências pode afetar a qualidade da conexão.
Segurança	Os adaptadores PLC geralmente oferecem recursos de segurança, como criptografia, para proteger a comunicação de dados transmitida pela rede elétrica.
Custo acessível	O PLC é geralmente considerado uma opção de custo acessível para fornecer acesso à internet, pois aproveita a infraestrutura elétrica existente.

Compatibilidade universal	A tecnologia PLC é compatível com a maioria dos dispositivos que podem ser conectados à rede por meio de uma conexão com fio, como computadores, impressoras, TVs inteligentes e sistemas de segurança.
Desafios ambientais	A qualidade da conexão PLC pode ser afetada por interferências causadas por dispositivos elétricos e circuitos elétricos ruidosos.

Radiodifusão

INCIDÊNCIA EM PROVA: baixíssima



Trata-se da tecnologia que permite o acesso à internet banda larga via radiofrequência. As ondas de rádio, em sua maior parte, são omnidirecionais, isto é, quando uma antena transmite ondas de rádio, elas se propagam em todas as direções em broadcast. Elas podem percorrer grandes distâncias e podem atravessar paredes, não necessitando que antenas transmissoras estejam completamente alinhadas.

No entanto, não pode haver grandes obstáculos entre o emissor e o receptor de sinal, como montanhas. **Trata-se de uma boa alternativa quando não é possível utilizar uma rede cabeada**, no entanto existem também diversas desvantagens: ondas de rádio podem sofrer interferências de outras ondas; a geografia entre as antenas pode ser um impeditivo; está bastante sujeito a intempéries climáticas como tempestades e vendavais; entre outros.

Não é muito utilizado em meios urbanos, mas é uma boa alternativa para meios rurais, onde cabos não estão disponíveis. Vejamos as principais características de redes de radiodifusão:

radiodifusão	Descrição
Transmissão por Ondas de rádio	A transmissão de dados é realizada por meio de ondas de rádio, que são transmitidas por uma estação base para receptores localizados nas residências ou empresas dos usuários.
Sem fios	A radiodifusão é uma tecnologia sem fio, o que significa que não requer cabos físicos para conectar os usuários à internet. Isso a torna especialmente útil em áreas geograficamente desafiadoras.
Ampla cobertura	As redes de radiodifusão podem oferecer uma cobertura mais ampla em comparação com outras tecnologias sem fio, como redes de celular. Isso as torna adequadas para áreas rurais e afastadas.
Provedores de serviço específicos	A maioria dos serviços de radiodifusão de internet é fornecida por provedores de serviço específicos que possuem e operam a infraestrutura de transmissão de rádio.
Equipamento do cliente	Os usuários precisam de equipamentos receptores, como antenas ou roteadores específicos para se conectarem à rede de radiodifusão. Esses equipamentos podem ser instalados em telhados, torres ou locais elevados para melhorar a recepção do sinal.
Latência e velocidade	A latência e a velocidade da conexão de radiodifusão podem variar dependendo da qualidade do sinal e do congestionamento da rede. Em alguns casos, a latência pode ser mais alta do que em tecnologias com fio, como fibra óptica.
Largura de banda limitada	As redes de radiodifusão podem ter largura de banda limitada, o que pode afetar a capacidade de suportar múltiplos dispositivos e aplicativos simultaneamente.
Custos variáveis	Os custos de assinatura de serviços de radiodifusão podem variar dependendo da localização do usuário e do provedor de serviço.

	específico. Além disso, os custos de equipamento inicial também podem ser relevantes.
Necessidade de linha de visão direta	Em algumas configurações de radiodifusão, pode ser necessário ter uma linha de visão direta entre a antena receptora e a torre de transmissão para obter uma boa qualidade de sinal.
Usos diversos	Além de fornecer acesso à internet, a tecnologia de radiodifusão é usada em comunicações de rádio em duas direções, como rádio por satélite, que pode ser usada para acesso à internet e transmissão de conteúdo de áudio e vídeo.

#VamosPraticar#

(FUNIVERSA / CEB – 2010) A transmissão de sinais está condicionada à qualidade do meio de comunicação, que pode variar de acordo com as condições físicas a que esteja sujeito. Parâmetros como velocidade de transmissão, atraso e variação no atraso de pacotes, taxa de erro são afetados quando há perda na qualidade do meio físico. Assinale a alternativa que apresenta o meio físico que sofre maiores interferências das variações climáticas, como acúmulo de nuvens e precipitações.

- a) Fibra óptica
- b) Cabo de par trançado
- c) Enlace de rádio
- d) Cabo coaxial
- e) Rede elétrica

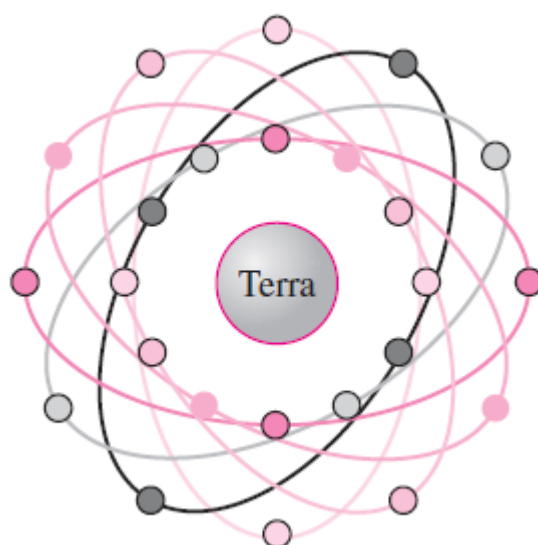
Comentários: quem sofre maiores interferências com acúmulo de nuvens e precipitações é o enlace de rádio (Letra C).

#VamosPraticar#

Satélite

INCIDÊNCIA EM PROVA: baixíssima

Uma rede via satélite é uma combinação de nós que fornecem comunicação de um ponto a outro na Terra. Nesse contexto, um nó pode ser um satélite, uma estação terrestre ou o terminal/telefone de um usuário final. *Vocês sabiam que é possível utilizar a Lua como satélite?* Não há nenhum problema, mas prefere-se o emprego de satélites artificiais que permitem a instalação de equipamentos eletrônicos para regenerar o sinal que perdeu intensidade durante seu trajeto.



Outra restrição no emprego de satélites naturais são suas distâncias até o nosso planeta, que criam um longo retardo nas comunicações. Os satélites podem oferecer recursos de transmissão de/para qualquer ponto da Terra, não importando sua distância. Essa vantagem possibilita a disponibilização de comunicação de alto padrão em partes subdesenvolvidas do mundo sem exigir grandes investimentos em infraestrutura terrestre. *Como assim, Diego?*

Galera, existem algumas regiões que não existe absolutamente nenhuma infraestrutura – nem sequer via radiodifusão. Um nômade em um deserto, um navio no meio do oceano, um cientista no meio da floresta amazônica – não existe infraestrutura! **Como vantagem, ele permite o acesso à internet de qualquer lugar do planeta em broadcast; por outro lado, ele é bastante caro e também está sujeito a intempéries climáticas.**

satélite	Descrição
Transmissão via satélite	A tecnologia de satélite envolve o uso de satélites de comunicação em órbita da Terra. Esses satélites atuam como retransmissores de sinais, permitindo que os provedores de serviço transmitam dados de internet para os usuários e vice-versa.
cobertura global	Uma das principais vantagens da tecnologia de satélite é sua capacidade de fornecer cobertura global. Isso significa que ela pode ser usada em áreas rurais, remotas ou em locais onde a infraestrutura terrestre é limitada.
Equipamento do usuário	Os usuários precisam de equipamentos específicos para se conectarem à internet via satélite. Isso inclui uma antena parabólica e um modem via satélite. A antena parabólica é instalada no local do usuário e aponta para o satélite de comunicação.

Latência	Possui latência relativamente alta, porque os sinais de internet devem viajar para o satélite e depois retornar à Terra. Embora a latência venha sendo reduzida, ainda pode ser notada em aplicações sensíveis à latência, como jogos online em tempo real.
Velocidade variável	A velocidade da conexão via satélite pode variar dependendo da oferta do provedor de serviço e das condições atmosféricas. Em geral, as conexões de satélite podem oferecer velocidades que variam de moderadas a muito altas, dependendo do plano escolhido.
Custo	Os custos de assinatura de serviços de satélite podem variar e tendem a ser mais caros do que os de tecnologias de acesso à internet por cabo ou DSL. Além disso, o equipamento inicial, como a antena parabólica e o modem, também tem um custo associado.
Uso em locais remotos	A tecnologia de satélite é especialmente útil em locais remotos, onde outras opções de banda larga não estão disponíveis.
Redes vsat	Em algumas configurações empresariais, a tecnologia de satélite é usada em redes de satélite de pequena abertura de terminal de terra (VSAT). Isso permite a conectividade de dados de alta velocidade para empresas e locais em áreas remotas.
Aplicações diversas	Além do acesso à internet, a tecnologia de satélite é usada em comunicações globais, TV via satélite e comunicações por satélite em locais sem infraestrutura de telecomunicações.

Telefonia Móvel

INCIDÊNCIA EM PROVA: baixíssima

Trata-se da tecnologia projetada para estabelecer comunicação entre duas unidades móveis, denominadas Estações Móveis; ou entre uma unidade móvel e outra fixa, normalmente chamada Unidade Terrestre. Um provedor de serviços tem de ser capaz de localizar e rastrear uma unidade que faz chamada, alocar um canal à chamada e transferir o canal de uma estação rádio base a outra à medida que o usuário que faz a chamada deixa a área de cobertura.

Para permitir esse rastreamento, cada área de serviço é dividida em pequenas regiões chamadas células e cada célula contém uma antena (por essa razão, é chamada de telefonia celular). O tamanho da célula não é fixo e pode ser aumentado ou diminuído, dependendo da população da região. **A telefonia celular encontra-se agora na quinta geração, porém vai demorar um pouco até chegar aos brasileiros.** Vejamos as principais gerações de telefonia celular:

- **Primeira Geração (1G):** a primeira geração foi projetada para comunicação de voz usando sinais analógicos. Introduzida em 1982 e encerrada em 1990, era usada apenas para serviços de voz e baseado em tecnologia chamada Advanced Mobile Phone System (AMPS).
- **Segunda Geração (2G):** a segunda geração de redes móveis foi a primeira a utilizar a tecnologia digital para transmissão de voz. As principais tecnologias 2G incluíam o GSM (Sistema Global para Comunicações Móveis) e o CDMA (Acesso Múltiplo por Divisão de Código).
- **Segunda Geração (2,5G):** também chamada de GPRS (Serviço de Rádio Geral), essa geração representou uma melhoria nas redes 2G com maior capacidade de transferência de dados e suporte limitado à internet móvel.
- **Terceira Geração (3G):** as redes 3G introduziram a transmissão de voz e vídeo digital, bem como a capacidade de acesso à internet móvel em alta velocidade. Tecnologias como o UMTS (Sistema Universal de Telecomunicações Móveis) e o CDMA2000 foram comuns.
- **Quarta Geração (4G):** o 4G foi projetado para oferecer velocidades de internet móvel significativamente mais rápidas em comparação com as gerações anteriores. Tecnologias, como o LTE (Evolução a Longo Prazo) e o WiMAX, foram amplamente utilizadas.
- **Quinta Geração (5G):** baseado na tecnologia OFDM, trata-se da próxima geração de telefonia celular. Começou a ser implantada em alguns lugares ao final de 2018 e possuem uma largura de banda maior, proporcionando maiores velocidades de download.

Telefonia móvel	Descrição
-----------------	-----------

Redes de comunicação sem fio	A tecnologia de telefonia móvel é baseada em redes de comunicação sem fio, como 3G, 4G (LTE) e 5G. Essas redes são projetadas para fornecer conectividade à internet em áreas urbanas e rurais, bem como em movimento.
Smartphones e dispositivos móveis	Os dispositivos móveis, como smartphones e tablets, são usados para acessar a internet por meio de redes móveis. Eles são equipados com módulos de comunicação que suportam diferentes gerações de redes, como 3G, 4G e 5G.
Cobertura ampla	As redes de telefonia móvel geralmente oferecem uma ampla cobertura geográfica. Isso significa que os usuários podem acessar a internet em uma variedade de locais, desde áreas urbanas densamente povoadas até áreas rurais remotas.
Velocidade variável	A velocidade da conexão à internet por telefonia móvel pode variar dependendo da geração da rede e das condições locais. As redes 4G e 5G oferecem velocidades mais altas em comparação com as redes 3G.
Planos de dados móveis	Os usuários normalmente adquirem planos de dados móveis de seus provedores de serviços. Esses planos podem variar em termos de dados disponíveis, velocidade e preço.
Wi-fi	Além da conectividade de rede móvel, muitos dispositivos móveis também suportam conexões Wi-Fi. Isso permite que os usuários se conectem a redes locais de alta velocidade, como as disponíveis em residências, cafés, aeroportos e locais públicos.
Aplicações móveis	Os smartphones e tablets executam uma variedade de aplicativos que facilitam o acesso à internet. Isso inclui navegadores da web, aplicativos de mídia social, serviços de e-mail, aplicativos de streaming de vídeo e muito mais.
Roaming internacional	Alguns planos de telefonia móvel oferecem a capacidade de acessar a internet enquanto viajam internacionalmente. Isso pode ser útil para turistas e viajantes de negócios.
Acesso em movimento	A capacidade de acessar a internet em movimento é uma das principais vantagens da tecnologia de telefonia móvel. Os usuários podem acessar

	informações, navegar na web, verificar e-mails e muito mais enquanto estão em trânsito.
5g e o futuro	A introdução da tecnologia 5G representa um avanço significativo na velocidade e capacidade de conexão da telefonia móvel. Isso possibilita uma variedade de novas aplicações, como Internet das Coisas (IoT) e realidade aumentada (AR).

1.14 Redes de Computadores - Parte 1 - Resumo

Resumo

REDES DE COMPUTADORES

DEFINIÇÃO de rede de computadores

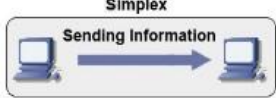
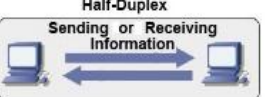
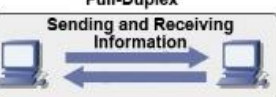
Uma rede é um conjunto de terminais, equipamentos, meios de transmissão e comutação que interligados possibilitam a prestação de serviços.

TIPOS DE CONEXÃO/ENLACE

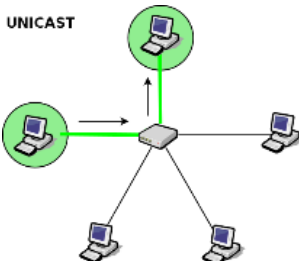
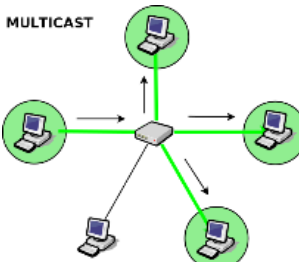
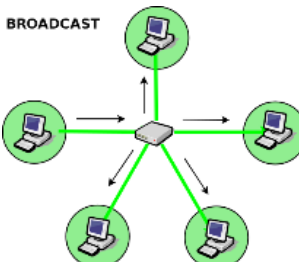
TIPO DE CONEXÃO	DESCRIÇÃO
PONTO-A-PONTO	Conexão que fornece um link dedicado entre dois dispositivos.
PONTO-MULTIPONTO	Conexão que fornece um link compartilhado entre mais de dois dispositivos.

DIREÇÕES DE TRANSMISSÃO

TIPO	REPRESENTAÇÃO	DESCRIÇÃO
------	---------------	-----------

SIMPLEX		Uma comunicação é dita simplex quando há um transmissor de mensagem, um receptor de mensagem e esses papéis nunca se invertem no período de transmissão.
HALF-DUPLEX		Uma comunicação é dita half-duplex quando temos um transmissor e um receptor, sendo que ambos podem transmitir e receber dados, porém nunca simultaneamente.
FULL-DUPLEX		Uma comunicação é dita full-duplex quando temos um transmissor e um receptor, sendo que ambos podem transmitir e receber dados simultaneamente.

MODOS DE TRANSMISSÃO

TIPO	REPRESENTAÇÃO	DESCRIÇÃO
UNICAST		Uma mensagem só pode ser enviada para um destino. Grosso modo, quando você envia uma mensagem no Whatsapp para uma pessoa específica, você está enviando uma mensagem unicast.
MULTICAST		Uma mensagem é enviada para um grupo de destino. Grosso modo, quando você cria uma lista de transmissão no Whatsapp com um grupo de pessoas e os envia uma mensagem, você está enviando uma mensagem multicast.
BROADCAST		Uma mensagem é enviada para todos os destinos. Grosso modo, quando você cria uma lista de transmissão no Whatsapp com todos os seus contatos e os envia uma mensagem, você está enviando uma mensagem broadcast.

CLASSIFICAÇÃO DE REDES: QUANTO À DIMENSÃO

TIPO	SIGLA	DESCRIÇÃO	DISTÂNCIA
PERSONAL AREA NETWORK	PAN	Rede de computadores pessoal (celular, tablet, notebook, entre outros).	De alguns centímetros a alguns poucos metros.
LOCAL AREA NETWORK	LAN	Rede de computadores de lares, escritórios, prédios, entre outros.	De algumas centenas de metros a alguns quilômetros.
METROPOLITAN AREA NETWORK	MAN	Rede de computadores entre uma matriz e filiais em uma cidade.	Cerca de algumas dezenas de quilômetros.
WIDE AREA NETWORK	WAN	Rede de computadores entre cidades, países ou até continentes.	De algumas dezenas a milhares de quilômetros.

CLASSIFICAÇÃO DE REDES: QUANTO À ARQUITETURA

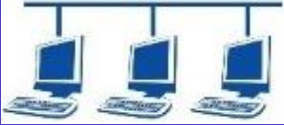
TIPO de rede	DESCRIÇÃO
PONTO A PONTO	Também chamada de Rede Par-a-Par, é o modelo de rede mais simples de ser montado. Nesse modelo, todas as máquinas podem compartilhar dados e periféricos umas com as outras. Essas redes são comuns em residências e entre filiais de empresas, porque demandam um baixo custo, são facilmente configuráveis e possibilitam altas taxas de velocidade de conexão.

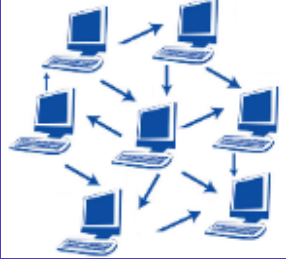
**CLIENTE/
SERVIDOR**

É um modelo de redes mais complexo, porém mais robusto e confiável. Nesse modelo, existe uma máquina especializada, dedicada e geralmente remota, respondendo rapidamente aos pedidos vindos dos demais computadores da rede – o que aumenta bastante o desempenho de algumas tarefas. É a escolha natural para redes grandes, como a Internet – que funciona tipicamente a partir do Modelo Cliente/Servidor.

CLASSIFICAÇÃO DE REDES: QUANTO À TOPOLOGIA

TIPO DE TOPOLOGIA	DESCRIÇÃO
FÍSICA	Exibe o layout (disposição) dos links e nós de rede.
LÓGICA	Exibe o fluxo ou percurso dos dados na rede.

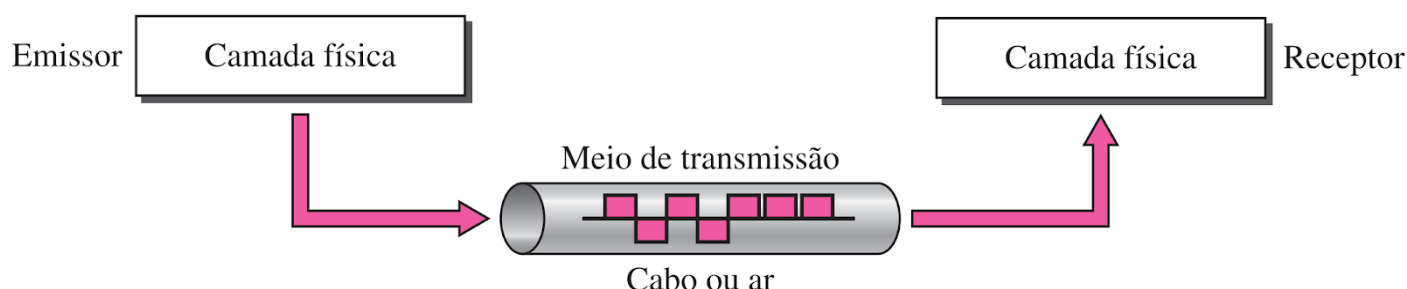
TIPO	REPRESENTAÇÃO	DESCRIÇÃO
BARRAMENTO (BUS)		Todas as estações ficam ligadas ao mesmo meio de transmissão, isto é, um único cabo (chamado backbone) em que os nós se ligam através de conectores. Há maior facilidade na instalação e economia de cabeamento, mas não há isolamento de falhas – uma ruptura no cabo implica a interrupção da comunicação.
ANEL (RING)		Cada dispositivo possui uma conexão ponto-a-ponto com outros dois dispositivos conectados lado a lado, e fazendo uso de uma comunicação com transmissão unidirecional (simplex). Nesse caso, a mensagem circula o anel, sendo regenerada e retransmitida a cada nó, passando pelo dispositivo de destino que copia a informação enviada, até retornar ao emissor original. Nesse momento, o link é liberado para que possa ser utilizado pelo nó seguinte.

ESTRELA (STAR)		As estações estão ligadas a um nó central controlador, pelo qual passam todas as mensagens, não havendo tráfego direto entre os dispositivos. O enlace entre estações e o nó central é Ponto-a-Ponto. É a topologia mais usada atualmente por facilitar a adição de novas estações e a identificação ou isolamento de falhas, em que – se uma conexão se romper – não afetará a comunicação de outras estações.
MALHA (MESH)		Cada estação possui um link ponto a ponto dedicado geralmente com transmissão bidirecional (full duplex) entre cada uma das demais estações. Em outras palavras, todos os computadores estão interligados entre si, de modo que caso haja uma ruptura em algum cabo, não cai a rede inteira, somente o nó conectado a esse cabo.

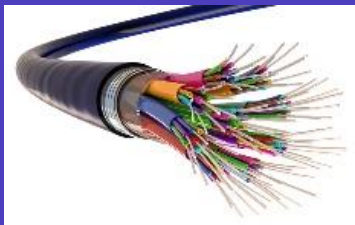
TOPOLOGIA física	DIREÇÃO DE TRANSMISSÃO	Tipo de ENLACE	MODOS DE TRANSMISSÃO
Barramento	Half-Duplex	Multiponto	Broadcast
Anel	Simplex	Ponto-a-Ponto	Broadcast
Estrela	Half-Duplex, se usar Hub; caso contrário Full-Duplex	Ponto-a-Ponto	Broadcast, se usar Hub; caso contrário, Unicast, Multicast ou Broadcast
Malha	Depende	Ponto-a-Ponto	Unicast, Multicast ou Broadcast

MEIOS DE TRANSMISSÃO

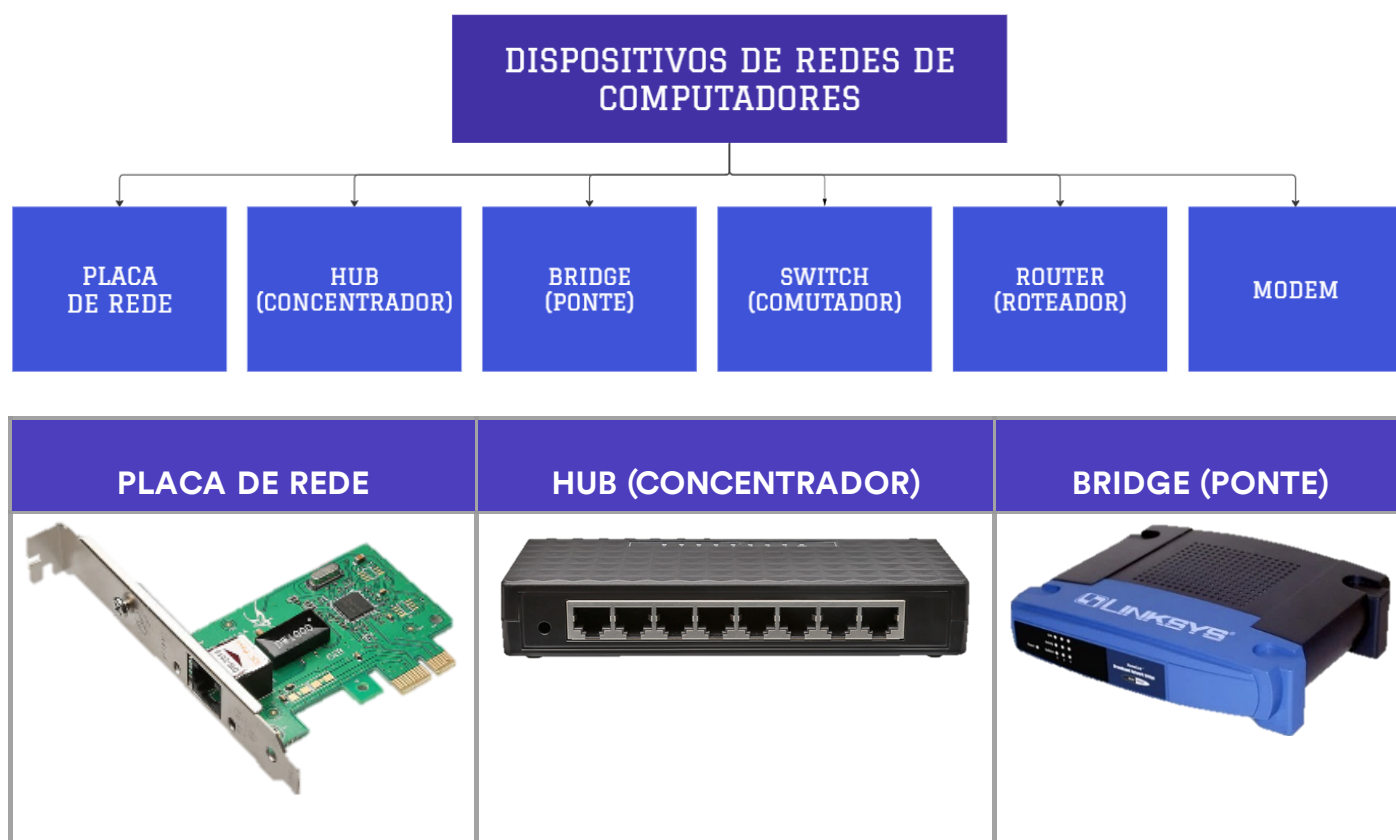
TIPO DE MEIO	DESCRIÇÃO
GUIADO	Trata-se da transmissão por cabos ou fios de cobre, onde os dados transmitidos são convertidos em sinais elétricos que propagam pelo material condutor. Exemplo: cabos coaxiais, cabos de par traçado, fibra óptica, entre outros.
NÃO-GUIADO	Trata-se da transmissão por irradiação eletromagnética, onde os dados transmitidos são irradiados através de antenas para o ambiente. Exemplo: ondas de rádio, microondas, infravermelho, bluetooth e wireless.



TIPO	REPRESENTAÇÃO	DESCRIÇÃO
CABO COAXIAL		Consiste em um fio central de cobre, envolvido por uma blindagem metálica. Isolantes de plástico flexível separam os condutores internos e externos e outras camadas do revestimento que cobrem a malha externa. Esse meio de transmissão é mais barato, relativamente flexível e muito resistente à interferência eletromagnéticas graças à malha de proteção que possui. Esse cabo cobre distâncias maiores que o cabo de par trançado e utiliza um conector chamado BNC.

CABO DE PAR TRANÇADO		Consiste de quatro pares de fios trançados blindados ou não, e envolto de um revestimento externo flexível. Eles são trançados para diminuir a interferência eletromagnética externa e interna – quanto mais giros, maior a atenuação. Este é o cabo mais utilizado atualmente por ser o mais barato de todos e ser bastante flexível. Esse cabo cobre distâncias menores que o cabo coaxial e utiliza um conector chamado RJ-45 (Memorizem!).
CABO DE FIBRA ÓPTICA		Consiste em uma Casca e um Núcleo (de vidro) para transmissão de luz. Possui capacidade de transmissão virtualmente infinita, é imune a interferências eletromagnéticas e consegue ligar distâncias maiores sem a necessidade de repetidores. Como desvantagens, podemos dizer que é incapaz de fazer curvas acentuadas, além de ter um custo de instalação e manutenção muito alto em relação ao par trançado. Há dois tipos de fibra: Monomodo e Multimodo.

Equipamentos de redes



Equipamento de rede de comunicação bidirecional (entrada e saída de dados) conectado à placa-mãe do computador. Toda placa de rede possui um número identificador chamado Endereço MAC (48 Bits).	Dispositivo de rede capaz de aumentar o alcance de uma rede local por meio da regeneração de sinais. É capaz de trabalhar apenas com broadcast, isto é, ao receber um pacote de dados, distribui para todas as máquinas da rede.	Equipamento capaz de separar uma rede em segmentos menores, reduzindo as chances de colisões quando várias máquinas desejam transmitir dados ao mesmo tempo. São dispositivos capazes de enviar dados para máquinas específicas.
SWITCH (COMUTADOR)	ROUTER (ROTEADOR)	modem
		
Equipamento semelhante às Bridges, no entanto possuem mais portas. Em contraste com hubs, são capazes de enviar transmitir dados para máquinas específicas (unicast ou multicast). Por segmentarem a rede, reduzem as colisões e diminuem o fluxo de informações.	Equipamento que permite interligar redes distintas e são capazes de escolher as melhores rotas para transmissão de pacotes de dados. É responsável por interligar dispositivos de uma rede local (Ex: Computador, Notebook, Smartphone, Impressora, etc) à internet.	Equipamento capaz de converter sinais digitais em sinais analógicos e vice-versa, em geral por meio de uma linha telefônica. Os três modelos principais são: Acesso Discado; Modem ADSL; e Cable Modem.

Placas de rede	DESCRIÇÃO
----------------	-----------

DEFINIÇÃO	Trata-se de um dispositivo que permite que um computador se conecte a uma rede de computadores, seja por meio de cabo ou sem fio.
CAMADA OSI	Camada 2 (Enlace). Atenção: vamos estudar o que são as camadas OSI mais à frente.
VANTAGENS	Permite que um computador se conecte a redes locais e à internet; facilita a comunicação entre dispositivos em uma rede; e oferece a capacidade de transmissão e recepção de dados.
DESVANTAGENS	Em redes sem fio, a qualidade do sinal pode afetar o desempenho; e pode ser uma vulnerabilidade de segurança se não configurada corretamente.

hubs	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo que simplesmente repete os dados recebidos em uma porta para todas as outras portas (está em desuso atualmente).
CAMADA OSI	Camada 1 (Física).
VANTAGENS	Custo geralmente baixo; simplicidade de operação; adequado para redes muito pequenas.
DESVANTAGENS	Pode causar tráfego ineficiente e colisões de dados; pode levar à degradação do desempenho em redes maiores; não possui inteligência para direcionar pacotes apenas para o destino certo.

bridges	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo de rede utilizada para dividir uma rede em segmentos menores, reduzindo colisões e tráfego de rede desnecessário

	(está em desuso atualmente).
CAMADA OSI	Camada 2 (Enlace).
VANTAGENS	Filtra o tráfego, melhorando o desempenho; pode conectar diferentes tipos de redes (Ex: Ethernet e Wi-Fi); aumenta a segurança da rede, criando domínios de colisão separados.
DESVANTAGENS	Pode ser mais caro do que um hub simples; requer configuração e gerenciamento adequados; limitação da extensão da rede e a complexidade de gerenciamento em redes maiores.

switches	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo de rede projetado para encaminhar pacotes de dados com base nos Endereços MAC (Media Access Control).
CAMADA OSI	Camada 2 (Enlace).
VANTAGENS	Rápido encaminhamento de pacotes; reduz colisões na rede; segmenta o tráfego da rede em diferentes portas; suporta redes com fio e sem fio; melhora o desempenho da rede.
DESVANTAGENS	Mais caro do que um hub; requer configuração e gerenciamento adequados; pode ter uma curva de aprendizado para administradores de rede.

roteadores	DESCRIÇÃO
DEFINIÇÃO	Trata-se de um dispositivo de rede que filtra, encaminha e controla pacotes de dados entre redes, determinando a melhor rota com base em endereços IP.

CAMADA OSI	Camada 3 (Rede).
VANTAGENS	Roteia tráfego entre redes, permitindo conectividade inter-redes; ajuda a dividir redes em sub-redes para melhor organização e segurança.
DESVANTAGENS	Pode ser mais complexo de configurar em comparação com switches/hubs; pode ser um ponto único de falha se não houver redundância.

Modem	DESCRIÇÃO
DEFINIÇÃO	Dispositivo que modula e demodula sinais para permitir a comunicação digital através de meios analógicos, como linhas telefônicas.
CAMADA OSI	Camada 1 (Física) e 2 (Enlace).
VANTAGENS	Permitem a comunicação de dados através de redes analógicas; são amplamente utilizados para acesso discado à Internet; facilitam a conexão com redes de banda larga.
DESVANTAGENS	Velocidade de transmissão baixa comparada com tecnologias de banda larga; suscetíveis a ruídos em linhas telefônicas; largura de banda e capacidade de transmissão limitadas.

PADRÕES DE REDES

PADRÕES DE REDES OU ARQUITETURA DE INTERCONEXÃO

Trata-se de um conjunto de padrões de interconexão de redes de computadores.

PADRÃO	NOME
IEEE 802.3	Ethernet (LAN)
IEEE 802.5	Token Ring (LAN)
IEEE 802.11	Wi-Fi (WLAN)
IEEE 802.15	Bluetooth (WPAN)
IEEE 802.16	WiMAX (WMAN)
IEEE 802.20	Mobile-Fi (WWAN)

PADRÕES DE REDES: 802.3

PADRÃO ETHERNET (IEEE 802.3)

Padrão de interconexão atualmente em redes locais cabeadas baseada no envio de pacotes de dados – possui diversas variantes como Fast Ethernet, Gigabit Ethernet, 10G Ethernet, etc.

EVOLUÇÃO DOS PADRÕES ETHERNET

PADRÃO (CABO DE PAR TRANÇADO)	PADRÃO – TAXA máxima DE TRANSMISSÃO
Ethernet	10BASE-T / 10 Mbps
Fast Ethernet	100BASE-T / 100 Mbps
Gigabit Ethernet	1000BASE-T / 1000 Mbps
10G Ethernet	10GBASE-T / 10000 Mbps

Vantagens do padrão ethernet	Desvantagens do padrão ethernet
Trata-se de uma das tecnologias de rede mais amplamente adotadas em todo o mundo.	Em redes Ethernet compartilhadas, as colisões de dados podem ocorrer, diminuindo o desempenho.
É relativamente fácil configurar e implantar, tornando-as acessíveis a muitas organizações.	Pode ser desafiador de escalar para redes maiores ou mais complexas.
Equipamentos e infraestruturas são geralmente mais acessíveis do que algumas alternativas.	Podem requerer cabeamento mais complexo e dispendioso.
Oferece boas taxas de transferência de dados e largura de banda adequada para muitos casos de uso.	Em redes Ethernet não criptografadas, os dados podem ser mais vulneráveis à interceptação.
A maioria dos dispositivos é compatível com Ethernet, facilitando a conectividade.	Em redes congestionadas, o desempenho do Ethernet pode diminuir.
Tende a ter latência baixa, o que é importante para aplicativos sensíveis à latência.	Não é adequada para redes sem fio, o que pode ser um problema em ambientes móveis.

PADRÕES DE REDES: 802.5

PADRÃO TOKEN RING (IEEE 802.5)

Arquitetura de conexão redes locais cabeada atualmente em desuso. Possui comunicação unidirecional (simplex), arquitetura ponto-a-ponto e topologia lógica em anel.

Vantagens do padrão token ring	Desvantagens do padrão token ring
O Token Ring é altamente confiável devido à sua estrutura em anel, que evita colisões de dados.	A implementação inicial do Token Ring pode ser mais cara devido ao hardware específico.

A topologia do anel elimina colisões de dados, o que leva a uma transmissão de alta qualidade.	Requer configuração complexa e habilidades técnicas para instalação e manutenção.
O tempo de latência é baixo, pois os dispositivos podem transmitir quando possuem o token.	Menos flexível do que outras topologias, tornando difícil adicionar ou mover dispositivos.
Permite a priorização de tráfego, garantindo que dados críticos sejam transmitidos primeiro.	A taxa de transmissão é geralmente mais baixa em comparação com tecnologias mais recentes.
Pode ser escalado facilmente, adicionando ou removendo dispositivos do anel.	O Token Ring é um padrão em declínio, com pouca inovação e suporte em comparação com Ethernet.

Característica	Padrão Token ring	Padrão Ethernet
topologia	Usa uma topologia em anel, onde os dispositivos são conectados em círculo e os dados são transmitidos em sequência – um dispositivo após o outro.	Usa uma topologia em estrela ou em barramento. Os dispositivos são conectados a um hub ou switch central.
Desempenho	Oferece um desempenho consistente devido à ausência de colisões de dados. A largura de banda é dividida igualmente entre os dispositivos no anel.	Pode ter colisões de dados, especialmente em redes ocupadas. A largura de banda é compartilhada entre todos os dispositivos na rede.
Custo	Geralmente é mais caro devido ao hardware específico necessário, como conectores de cabo MAU (<i>Media Access Unit</i>).	Geralmente é mais econômico, pois o hardware é amplamente disponível e menos caro.
implementação	Requer configuração mais complexa, como a definição de endereços de estação e prioridades de token.	É mais fácil de implementar, com menos requisitos de configuração.

Escalabilidade	Pode ser menos flexível para adicionar ou remover dispositivos sem interromper a rede.	É escalável e permite adicionar dispositivos com facilidade, especialmente em redes comutadas.
popularidade	Foi popular nas décadas de 1980 e 1990, mas agora é menos comum, pois a Ethernet se tornou dominante.	É a tecnologia de rede mais amplamente usada e suportada, com constante evolução.

PADRÕES DE REDES: 802.11

PADRÃO WIRELESS (IEEE 802.11)

Arquitetura de conexão de redes locais sem fio que define um conjunto de padrões de transmissão e codificação para comunicações não cabeadas.

característica	Modo de operação Ad-hoc	Modo de operação infraestrutura
descrição	Comunicação direta entre equipamentos e válida somente naquele momento, conexão temporária, apresentando alcance reduzido (Ex: 5m).	Comunicação que faz uso de equipamento para centralizar fluxo da informação na WLAN (Ex: Access Point ou Hotspot) e permite um alcance maior (Ex: 500m).
Topologia de rede	Tipo de topologia de malha, onde cada dispositivo se conecta diretamente a outros dispositivos na rede.	Os dispositivos se conectam a um ponto de acesso central, como um roteador, que age como intermediário para encaminhar o tráfego.

Configuração de rede	Configurada sem a necessidade de um ponto de acesso central. Os dispositivos podem se comunicar diretamente uns com os outros.	Requer um ponto de acesso central (como um roteador) para gerenciar e encaminhar o tráfego na rede.
Flexibilidade	Mais flexível e útil em cenários onde não há acesso a uma infraestrutura de rede. Pode ser configurada rapidamente para conexões ponto a ponto.	Menos flexível em termos de implantação, pois depende de um ponto de acesso central. Ideal para redes com vários dispositivos em um único local.
Escalabilidade	Menos escalável para grandes redes devido à complexidade de gerenciar muitas conexões ponto a ponto.	Mais escalável para redes maiores, pois o ponto de acesso central gerencia eficientemente as conexões.
Segurança	Geralmente menos segura, pois não existe um ponto de controle central. As comunicações podem ser vulneráveis a ataques.	Mais segura, pois o ponto de acesso central pode implementar medidas de segurança, como criptografia e autenticação, em nome de todos os dispositivos.
Exemplos de utilização	Redes temporárias de curto prazo, comunicação direta entre dispositivos móveis (por exemplo, compartilhamento de arquivos entre smartphones).	Redes domésticas, redes empresariais, hotspots públicos e ambientes onde múltiplos dispositivos precisam se conectar a uma rede comum.

EVOLUÇÃO DO PADRÃO wi-fi (802.11) ^[19]

PADRÃO	FREQUÊNCIA	TAXA máxima DE TRANSMISSÃO
IEEE 802.11b	2.4 Ghz	11 Mbps
IEEE 802.11a	5.0 Ghz	54 Mbps

IEEE 802.11g	2.4 Ghz	54 Mbps
IEEE 802.11n	2.4 ou 5.0 Ghz	150, 300 até 600 Mbps
IEEE 802.11ac	5.0 Ghz	500 Mbps, 1 Gbps ou +
IEEE 802.11AX (wifi 6)	2.4 ou 5.0 Ghz	3.5Gbps a 14Gbps

Vantagens do padrão wi-fi	Desvantagens do padrão wi-fi
Permite conectividade sem fio, possibilitando o uso de dispositivos em movimento, como laptops e smartphones.	Redes sem fio estão suscetíveis a interferências de outros dispositivos e redes, afetando o desempenho.
Fácil instalação e expansão de redes sem fio, evitando a necessidade de cabos físicos.	As redes sem fio podem ser vulneráveis a invasões se as medidas de segurança, como criptografia, não forem implementadas adequadamente.
Geralmente mais econômico do que a instalação de cabos em locais com vários dispositivos.	A velocidade da rede sem fio pode ser mais lenta do que as redes com fio, especialmente em locais congestionados.
Oferece opções de configuração, como redes ad-hoc e infraestrutura, para atender a diversas necessidades.	A qualidade da conexão pode ser afetada por obstáculos físicos, distância do roteador e interferências.
Disponível em várias faixas de frequência, permitindo cobertura em diferentes distâncias.	Redes sem fio podem apresentar maior latência do que redes com fio, o que pode ser crítico para algumas aplicações.

PADRÕES DE REDES: 802.15**PADRÃO BLUETOOTH (IEEE 802.15)**

O Padrão Bluetooth tem o objetivo de integrar equipamentos periféricos. Utilizado em Rede WPAN (Wireless PAN) – eles padronizam uma rede de baixo custo, curto alcance, baixas taxas de transmissão e sem fio.

PADRÃO BLUETOOTH – WPAN 802.15

CLASSE	Potência	DISTÂNCIA
1	100 mW	Até 100 Metros
2	2.5 mW	Até 10 Metros
3	1 mW	Até 1 Metro

Vantagens do padrão bluetooth	Desvantagens do padrão bluetooth
O padrão IEEE 802.15 é projetado para dispositivos de baixo consumo de energia, adequados para baterias.	As redes IEEE 802.15 têm alcance limitado, geralmente cobrindo apenas algumas dezenas de metros.
O padrão é ideal para comunicações de curto alcance, como sensores e dispositivos IoT em uma área próxima.	A largura de banda é limitada, o que a torna inadequada para aplicações que requerem alta taxa de transferência.
Permite a criação de redes de malha, onde dispositivos podem rotear dados entre si, aumentando a cobertura.	Pode ser afetada por interferências de outras redes sem fio e dispositivos, especialmente em ambientes lotados.

Usado em aplicações como IoT, sensores sem fio, automação residencial, dispositivos médicos e muito mais.	Não é a melhor opção para redes de grande escala, devido ao seu alcance limitado e limitações de largura de banda.
Substitui a necessidade de cabos em ambientes onde a conectividade com fio não é prática ou possível.	A segurança é uma preocupação, pois dispositivos dentro do alcance de uma rede IEEE 802.15 podem acessá-la.

PADRÕES DE REDES: 802.16

PADRÃO WIMAX (IEEE 802.16)

O Padrão WiMAX especifica um padrão sem fio de alta velocidade para Redes Metropolitanas (WMAN), criado por um consórcio de empresas para promover interoperabilidade entre equipamentos. Seu raio de comunicação com o ponto de acesso pode alcançar até cerca de 40 km, sendo recomendável para prover acesso à internet banda larga a empresas e residências em que o acesso ADSL ou HFC se torna inviável por questões geográficas.

Vantagens do padrão wimax	Desvantagens do padrão wimax
O IEEE 802.16 pode fornecer serviços de banda larga em uma ampla área geográfica, incluindo áreas urbanas e rurais.	A implantação de infraestrutura 802.16 pode ser cara, especialmente em áreas com baixa densidade populacional.
Oferece largura de banda significativa, o que é adequado para aplicações que exigem altas taxas de transferência de dados.	Apresenta latência mais alta em comparação com tecnologias como fibra óptica, o que pode afetar aplicativos sensíveis à latência.
Suporta mobilidade, permitindo a conexão de dispositivos em movimento, como em veículos ou trens de alta velocidade.	Pode ser suscetível a interferências de obstáculos, como edifícios altos e outros dispositivos sem fio na mesma faixa.

Comparado com tecnologias como DSL, o IEEE 802.16 pode oferecer conectividade de banda larga em áreas rurais remotas.	A compatibilidade entre diferentes implementações de 802.16 nem sempre é garantida, o que pode levar a problemas de interoperabilidade.
Oferece QoS para garantir que diferentes tipos de tráfego, como voz e vídeo, tenham desempenho adequado na rede.	A gestão eficaz do espectro é necessária para evitar interferências e garantir o desempenho da rede.

INTERNET

internet

A Internet é basicamente um vasto conjunto de redes de computadores diferentes que utilizam um padrão comum de comunicação e oferece um determinado conjunto de serviços.

Características	Web 1.0	Web 2.0	Web 3.0
Interatividade	Baixa	Alta	Muito Alta
conteúdo	Estático e somente leitura	Dinâmico, com feedback do usuário	Inteligente, com semântica
Usuários	Consumidores passivos	Produtores de conteúdos	Participantes ativos
Socialização	Ausente	Integração de redes sociais	Integração com IA e Internet das Coisas

Experiência do usuário	Limitada	Melhorada e personalizada	Altamente personalizada
Tecnologia	HTML	AJAX, APIs e RSS	IA e Aprendizado de Máquina
Exemplos	Sites estáticos de início da web	Redes sociais, blogs e wikis	Assistentes virtuais
Principais aplicações	Sites informativos e institucionais	Redes sociais e colaboração online	Assistentes virtuais e Internet das Coisas

DEEP WEB E DARK WEB

Características	Surface web	Deep web	Dark web
Acessibilidade	Acessível por mecanismos de busca e navegadores comuns.	Requer credenciais específicas ou URLs exclusivas.	Acessível apenas por redes criptografadas, como o Tor.
Conteúdo comum	Contém informações e sites disponíveis publicamente.	Inclui conteúdo não indexado por mecanismos de busca, como bancos de dados privados.	Contém conteúdo obscuro e frequentemente ilegal.
Anonimato	Não oferece anonimato especial para usuários.	Pode exigir credenciais de login, mas não enfatiza o anonimato.	Valoriza altos níveis de anonimato e segurança.

Conteúdo comercial	Amplamente usado para negócios, educação, entretenimento e informações públicas.	Inclui recursos protegidos por senha, como e-mails, serviços bancários online e redes corporativas.	Muitas vezes associada a atividades ilegais e conteúdo obscuro.
exemplos	Sites de notícias, blogs, redes sociais, sites de compras online.	E-mails privados, intranets corporativas, bancos de dados de bibliotecas.	Sites de venda de drogas, mercados negros, fóruns de hackers.

INTERNET DAS COISAS

INTERNET DAS COISAS

Trata-se de uma revolução tecnológica que se refere à conexão de dispositivos físicos e objetos do mundo real à internet. Esses dispositivos, também chamados de "coisas" na IoT, são integrados com sensores, software e outras tecnologias para coletar e trocar dados com outros dispositivos e sistemas pela internet.

Componentes	descrição
Dispositivos	São os elementos físicos que compõem a IoT, como sensores, atuadores e outros dispositivos conectados, como câmeras, medidores inteligentes, veículos e eletrodomésticos. Eles coletam dados do mundo real e podem executar ações com base nesses dados.
Tecnologias de comunicação	São os meios pelos quais os dispositivos IoT se comunicam entre si e com a nuvem. Isso pode incluir Wi-Fi, Bluetooth, 3G/4G/5G, Zigbee, LoRa, entre outros. As redes de comunicação são responsáveis pela transferência de dados dos dispositivos para a nuvem e vice-versa.

Sensores e Atuadores	Os sensores coletam informações do ambiente, como temperatura, umidade, localização, movimento e muito mais. Os atuadores são responsáveis por tomar ações, como ligar ou desligar um dispositivo. Eles são os olhos e as mãos da IoT.
Nuvem (cloud)	A nuvem é onde os dados coletados pelos dispositivos IoT são processados, armazenados e disponibilizados para acesso. Plataformas de nuvem fornecem recursos de computação, armazenamento e análise de dados em grande escala, tornando possível o processamento de grandes volumes de informações.

Vantagens	desvantagens
Varejistas podem fornecer bônus de fidelidade para clientes preferenciais.	A dependência de compras online pode custar empregos.
As cidades podem avaliar as necessidades futuras de transporte.	Os varejistas podem saber tudo o que você está comprando.
Indivíduos podem reduzir os custos de energia e dos sistemas de aquecimento residenciais.	Os indivíduos podem receber mais e-mails de spam.
Fabricantes podem reduzir a inatividade prevendo as necessidades de manutenção dos equipamentos.	Uma falha da rede pode ser catastrófica.
Os governos podem monitorar o ambiente.	As empresas que criam dispositivos vestíveis têm muitas informações pessoais sobre os usuários.

TECNOLOGIAS DE ACESSO

TECNOLOGIAS DE ACESSO À INTERNET

Referem-se aos métodos e infraestruturas utilizados para conectar dispositivos, como computadores, smartphones e outros equipamentos, à Internet. Essas tecnologias permitem que os dispositivos acessem os serviços e recursos disponíveis na World Wide Web e em outros serviços online. Existem várias tecnologias de acesso à Internet (Ex: Dial-Up, ADSL, HFC, Fibra Óptica, PLC, Radiodifusão, Satélite e Telefonia Móvel), e a escolha depende das necessidades e da disponibilidade em uma determinada região.

Níveis	Descrição
Isps nível 1	São os provedores de acesso à internet de nível mais alto na hierarquia. Eles não precisam comprar acesso à internet de outros provedores, pois possuem uma rede global de alta capacidade e trocam tráfego diretamente uns com os outros. Exemplos de provedores de Nível 1 incluem AT&T, Verizon, NTT Communications e CenturyLink. Eles têm uma presença global e fornecem acesso à internet em escala internacional. Imagine ISPs de Nível 1 como rodovias federais, como a Rodovia Presidente Dutra (BR-116). Essas rodovias cruzam continentes e países sem precisar pagar pedágio a outras estradas menores. Os provedores de Nível 1 constroem e mantêm essas "rodovias da internet" e interconectam-se diretamente para permitir um tráfego rápido e eficiente.
Isps nível 2	Estes são provedores de acesso à internet que não possuem redes globais como os Nível 1, mas ainda têm uma rede significativa em uma área geográfica específica. Eles geralmente compram acesso à internet de Nível 1 ISPs e podem vender serviços a ISPs de nível inferior ou a empresas e consumidores diretos. Exemplos de provedores de Nível 2 incluem Cogent, Orange, Charter, Deutsche Telekom, entre outros. ISPs de Nível 2 podem ser comparados a rodovias estaduais. Eles atendem a áreas geográficas maiores, como estados ou regiões inteiras. Essas rodovias estaduais se

	conectam às autoestradas globais (Nível 1) e podem cobrar pedágio por permitir que o tráfego flua entre essas grandes autoestradas e áreas locais.
ISP nível 3	São provedores regionais ou locais que não possuem redes globais. Eles compram acesso à internet de provedores de Nível 1 ou 2 para fornecer conectividade a empresas e consumidores em áreas geográficas específicas. Esses ISPs podem se concentrar em uma única cidade, região ou país. Alguns provedores de Nível 3 podem ser ISPs de acesso final, que fornecem serviços diretamente a residências e empresas locais. ISPs de Nível 3 são como as estradas locais e ruas em cidades. Eles atendem áreas geográficas muito específicas, como uma cidade ou bairro. Essas estradas locais se conectam às rodovias regionais (Nível 2) ou diretamente às autoestradas globais (Nível 1) e permitem que o tráfego alcance destinos locais.

Tecnologias de acesso	Descrição
Dial-up	Uma tecnologia de acesso discado à internet que utiliza a linha telefônica tradicional. É lenta e está em desuso na maioria das áreas.
Adsl	Uma tecnologia de acesso de banda larga que utiliza a linha telefônica para fornecer velocidades mais rápidas do que o dial-up.
Hfc	Uma tecnologia que combina fibra óptica e cabos coaxiais para fornecer serviços de internet de alta velocidade e TV a cabo.
Fibra óptica	Uma tecnologia de alta velocidade que utiliza cabos de fibra óptica para transmitir dados em alta velocidade por meio de pulsos de luz.
Plc	Utiliza a rede elétrica para transmitir dados, tornando a fiação elétrica existente uma rede de comunicação.
Radiodifusão	Utiliza ondas de rádio para transmitir dados. Pode incluir tecnologias como Wi-Fi e redes celulares.

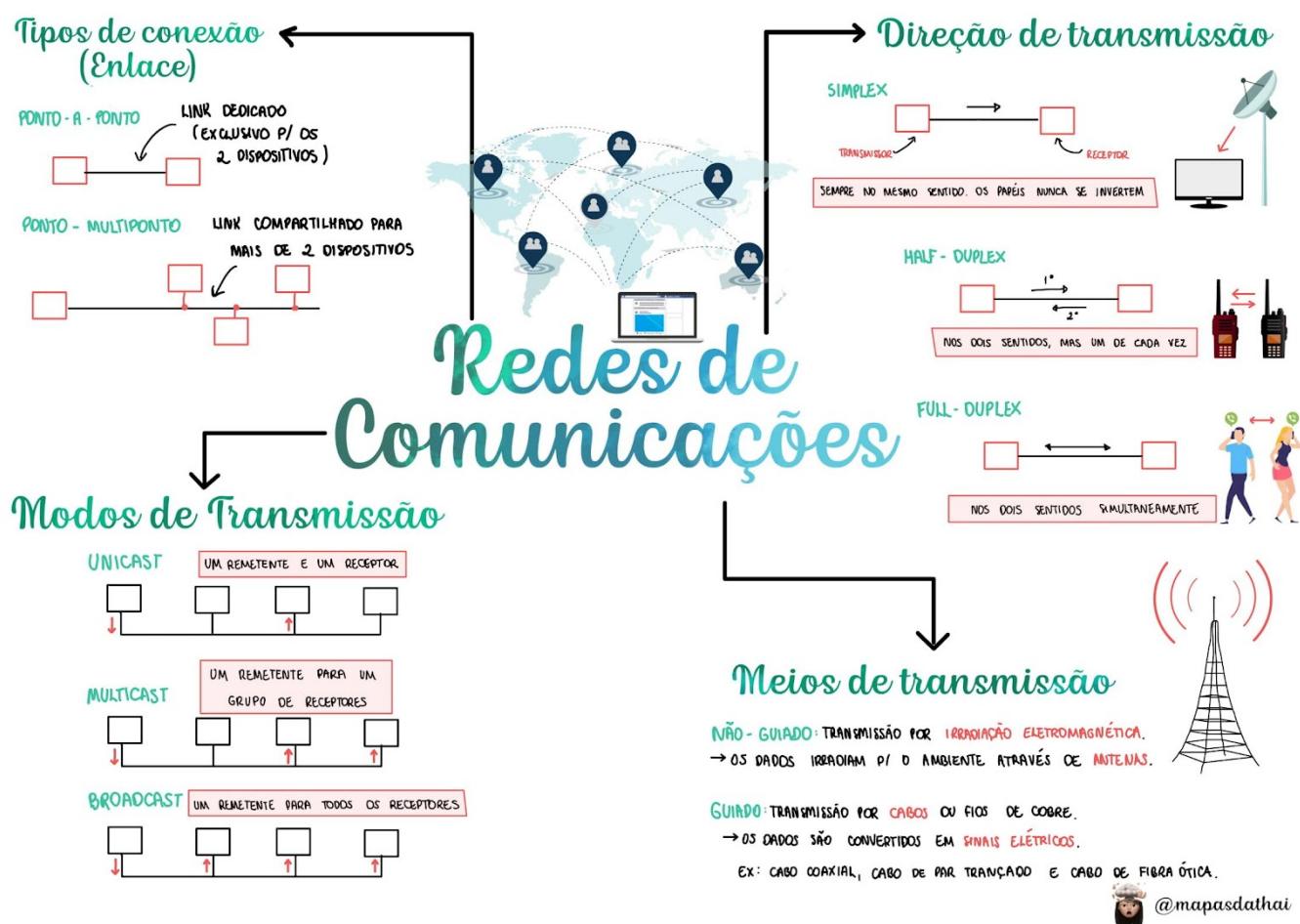
Satélite	Acesso à internet via satélite – os dados são enviados e recebidos por meio de satélites em órbita terrestre.
Telefonia móvel	Acesso à internet usando redes móveis (3G, 4G, 5G), permitindo a conexão em movimento a partir de dispositivos móveis.



PARA MAIS DICAS: www.instagram.com/professordiegocarvalho [20]

1.15 Mapa Mental - Redes de Computadores - Parte 1

Mapa Mental



Cabo coaxial

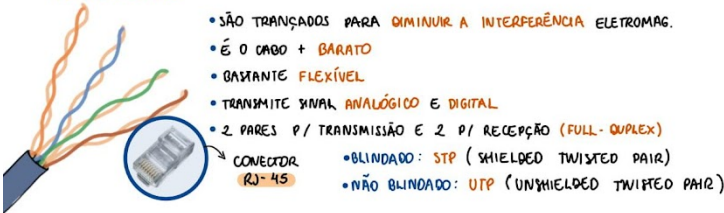


- MAIS BARATO
- RELATIVAMENTE FLEXÍVEL
- MUITO RESISTENTE (NÃO IMUNE) À INTERFERÊNCIA ELETROMAGNÉTICA
↳ GRAÇAS À MALHA/CAPA DE PROTEÇÃO
- COBRE DISTÂNCIAS MAIORES
- TAXA DE TRANSMISSÃO MENOR
- LARGURA DE BANDA MAIOR
- AINDA É USADO EM TELECOMUNICAÇÕES

Meios de Transmissão Guiados

Cabo de par trançado

QUATRO PARES DE FIOS TRANÇADOS, BLINDADOS OU NÃO, ENVOLTOS DE UM REVESTIMENTO EXTERNO FLEXÍVEL.



Cabo de Fibra Ótica

CONSISTE EM UMA CASCA E UM NÚCLEO (DE VIDRO) PARA TRANSMISSÃO DE LUZ.

- CAPACIDADE DE TRANSMISSÃO VIRTUALMENTE INDEFINIDA.
- IMUNE A INTERFERÊNCIAS ELETROMAGNÉTICAS
- LIGA DISTÂNCIAS MAIORES SEM NECESSIDADE DE UM REPETIDOR
- É INCAPAZ DE FAZER CURVAS ACENTUADAS
- ALTO CUSTO DE INSTALAÇÃO E MANUTENÇÃO

FIBRA MULTIMODO



- LEVA O FEIXE DE LUZ POR VÁRIOS MODOS/CAMINHOS
- DISTÂNCIA MENOR
- TAXA DE TRANSMISSÃO MENOR
- PRECISÃO MENOR
- DIÂMETRO MAIOR
- ALTO ÍNDICE DE REFRAÇÃO E ATENUAÇÃO
- CONSTRUÇÃO MAIS SIMPLES E MAIS BARATA
- USADA NAS LANs

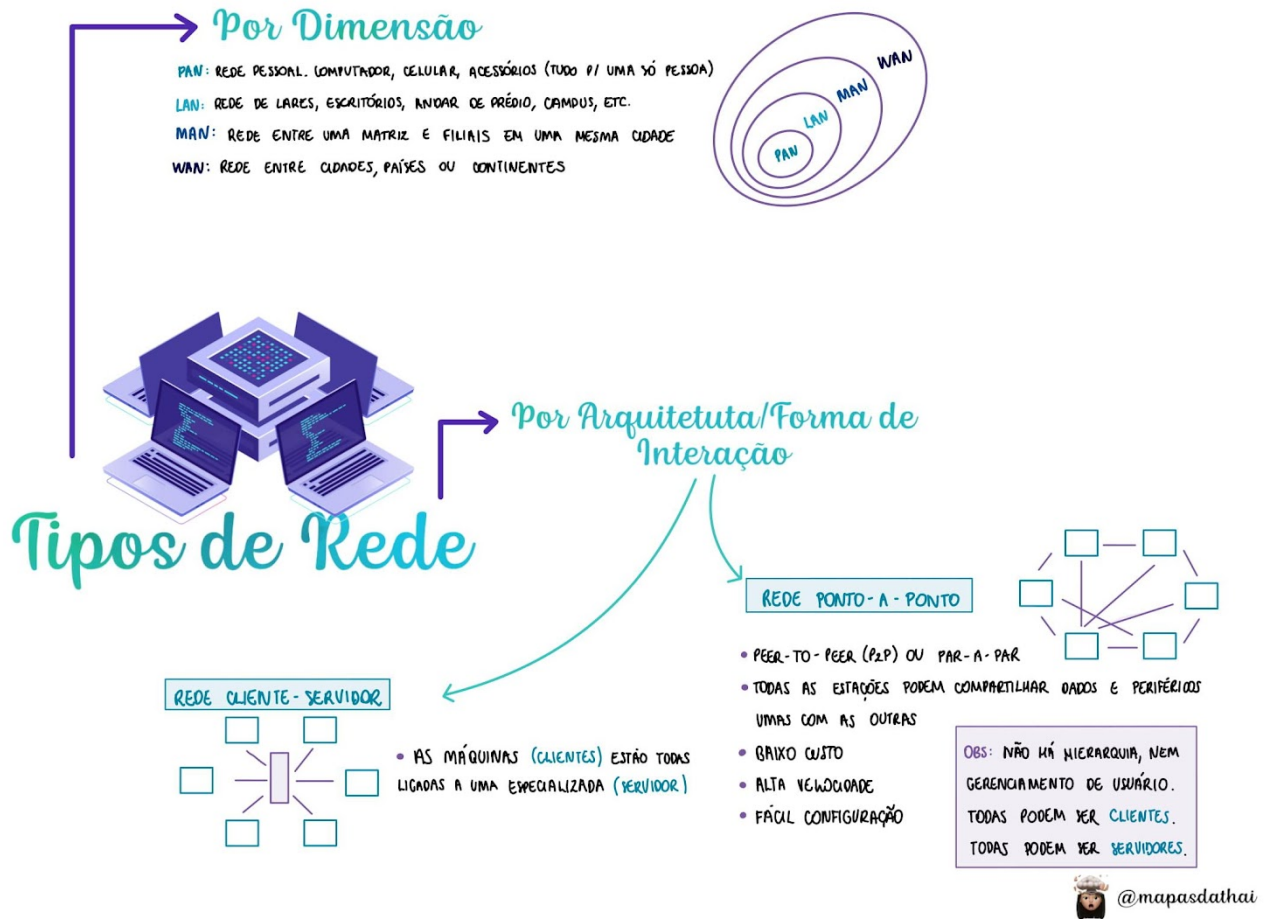
FIBRA MONOMODO

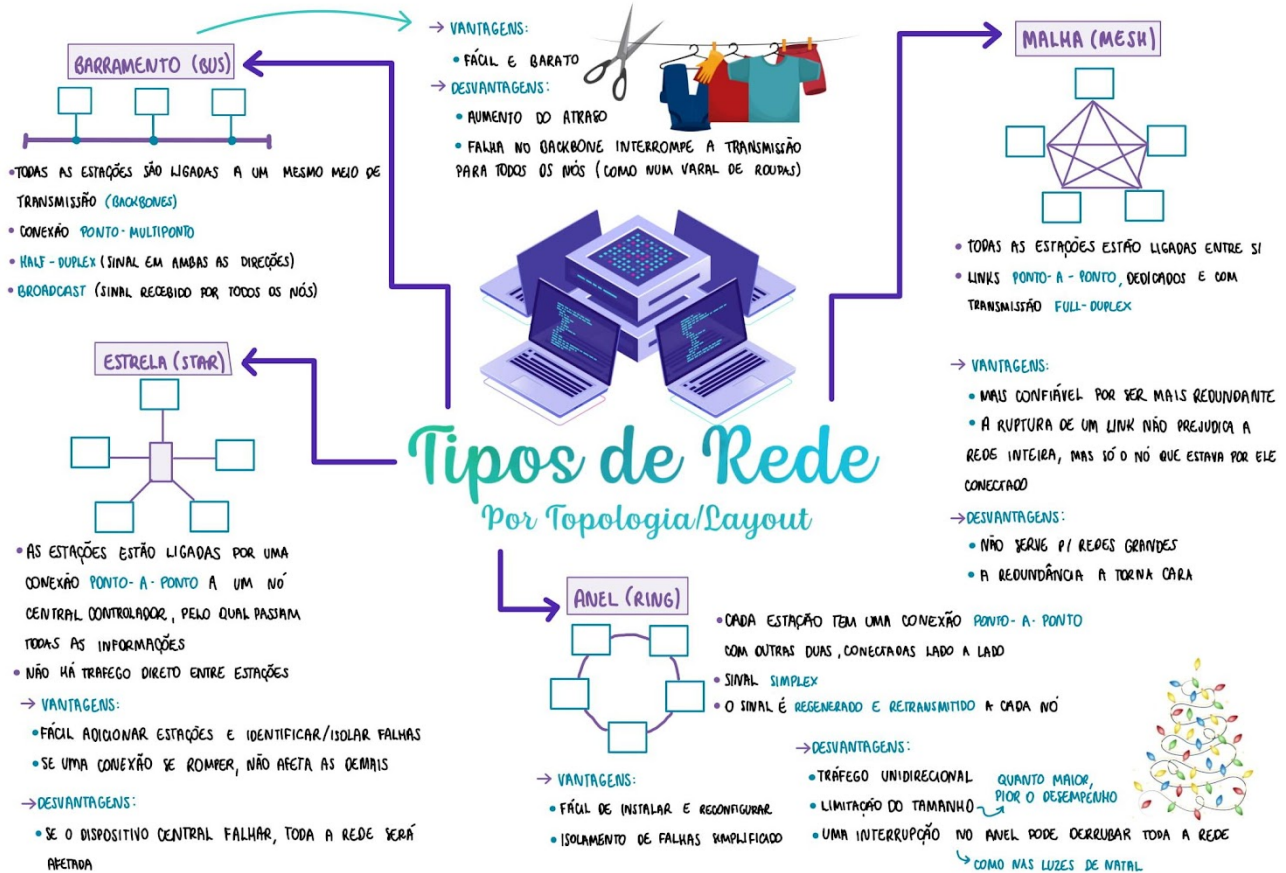


- LEVA O FEIXE DE LUZ POR UM ÚNICO MODO/CAMINHO
- DISTÂNCIA MAIOR
- TAXA DE TRANSMISSÃO MAIOR
- PRECISÃO MAIOR
- DIÂMETRO MENOR
- BAIXO ÍNDICE DE REFRAÇÃO E ATENUAÇÃO
- CONSTRUÇÃO MAIS COMPLEXA E MAIS CARA
- USADA NAS WANs

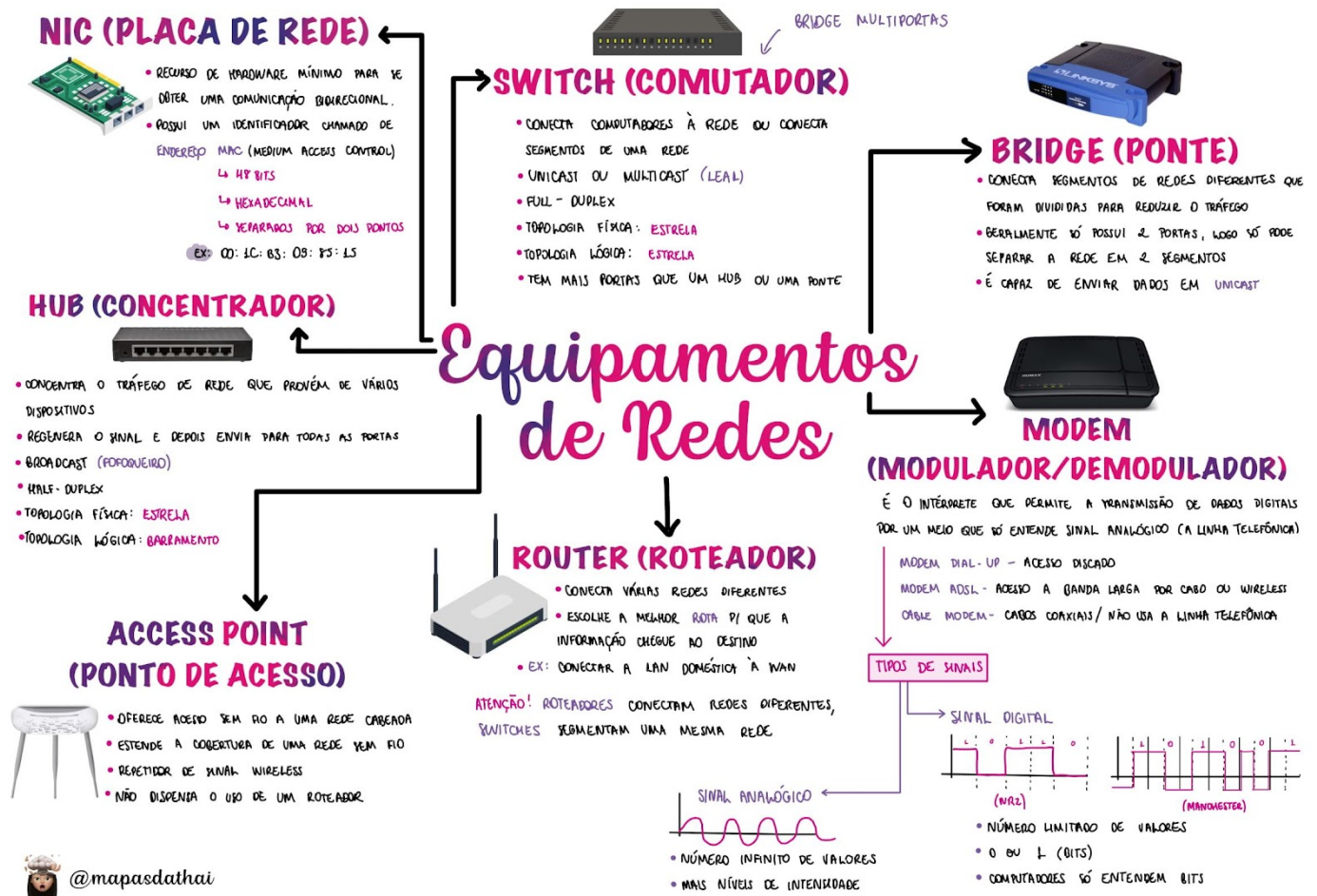


@mapasdathai





@mapasdathai

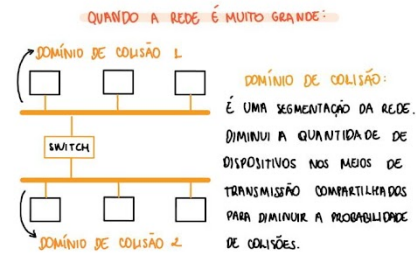


Ethernet

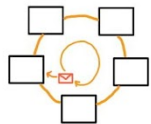
- PERMITE QUE 2 OU MAIS COMPUTADORES SE CONECTEM POR UMA LAN "CABEADA"



- **DESVANTAGEM:** TRÁFEGO ALTO PODE OCORRER COLISÃO = MENSAGENS ININTELIGÍVEIS
- **SOLUÇÃO:** ESPERAR EM VLÉNCIO DURANTE UM PERÍODO DE TEMPO ALEATÓRIO ANTES DE TENTAR NOVAMENTE



Token Ring



- PADRÃO CABEADO QUE ERA CONCORRENTE DO PADRÃO ETHERNET
- TOPOLOGIA EM ANEL / COMUNICAÇÃO SIMPLEX
- ARQUITETURA PONTO-A- PONTO
- NÃO TEM COLISÃO

EVOLUÇÃO DOS PADRÕES ETHERNET	
ETHERNET	10BASE-2 / 10Mbps / 185m
ETHERNET	10BASE-5 / 10Mbps / 500m
ETHERNET	10BASE-T / 10Mbps
FAST ETHERNET	100BASE-T / 100Mbps
GIGABIT ETHERNET	1000BASE-T / 1000Mbps
10G ETHERNET	10GBASE-T / 10.000Mbps

Padrões de Redes

IEEE 802.3	Ethernet (LAN)
IEEE 802.5	Token Ring (LAN)
IEEE 802.11	Wi-Fi (WLAN)
IEEE 802.15	Bluetooth (WPAN)
IEEE 802.16	WiMAX (WMAN)
IEEE 802.20	Mobile-Fi (WWAN)

Bluetooth

OBJETIVO: INTEGRAR EQUIPAMENTOS PERIFÉRICOS NA WPAN

- REDE DE BAIXO CUSTO
 - CURTO ALCANCE
 - BAIXAS TAXAS DE TRANSMISSÃO
 - FAIXA DE 2.4 GHz
 - CONECTA ATÉ 7 DISPOSITIVOS
 - ARQUITETURA MASTER / SLAVE
- MESTRE: PODE SE CONECTAR A VÁRIOS ESCRAVOS
ESCRAVO: SE CONECTA A APENAS UM MESTRE



Wireless



- SUA CONEXÃO UTILIZA ONDAS DE RÁDIO

EVOLUÇÃO DO PADRÃO WIRELESS		
PADRÃO	FREQUÊNCIA	TAXA DE TRANSMISSÃO
IEEE 802.11B	2.4GHz	11Mbps
IEEE 802.11A	5.0GHz	54Mbps
IEEE 802.11G	2.4GHz	54Mbps
IEEE 802.11N	2.4 ou 5.0GHz	150, 300 até 600Mbps
IEEE 802.11AC	5.0GHz	500Mbps, 1Gbps ou +

OBSERVAÇÕES:

- 802.11B e 802.11A NÃO SÃO EVOLUÇÃO UM DO OUTRO, ELES SURTIRAM SIMULTANEAMENTE
- O 802.11B ENTROU NO MERCADO PRIMEIRO
- O 802.11N É DUAL-BAND (PERMITE DUAS BANDAS DE FREQUÊNCIA)



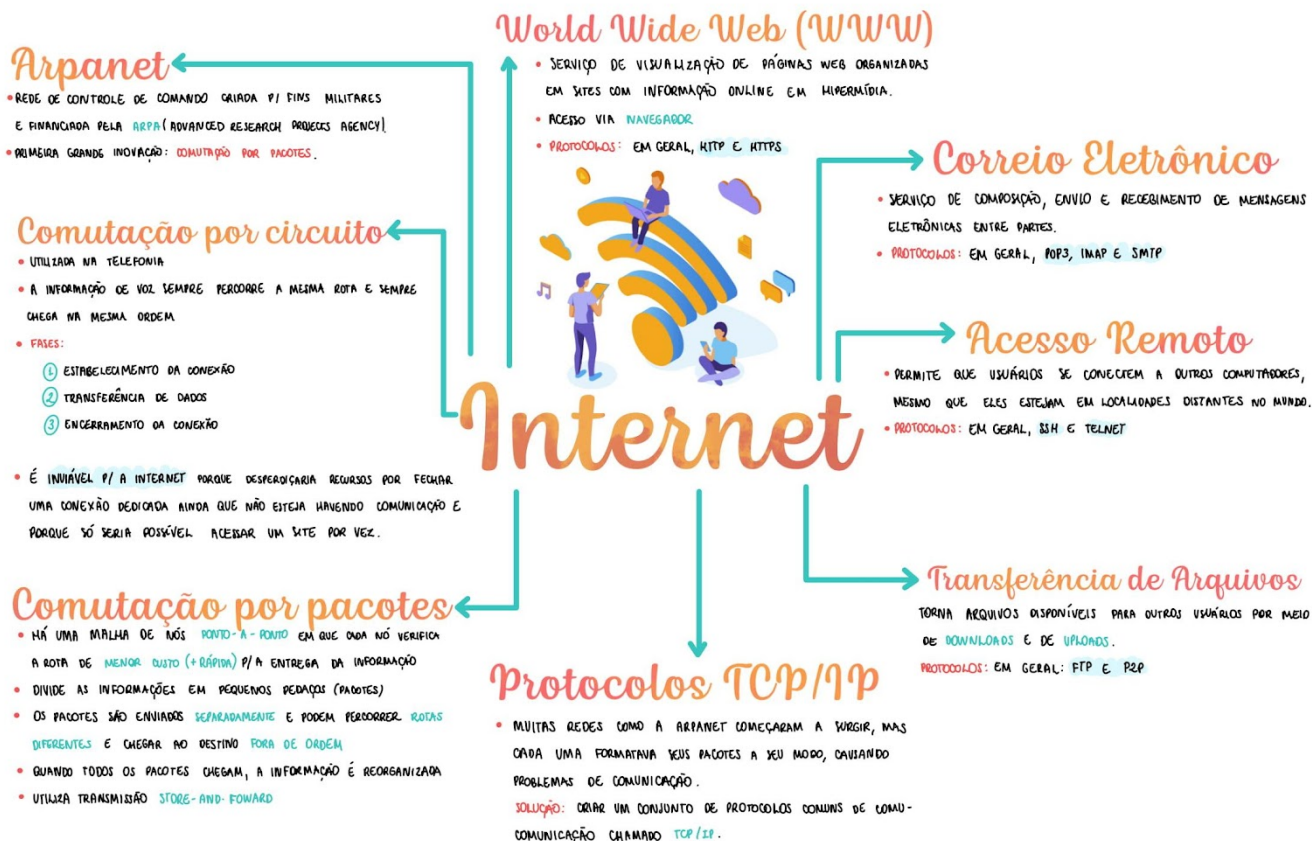
- BASEADA NO PADRÃO WIRELESS 802.11
- CONEXÃO POR PONTOS DE ACESSO (HOT SPOT)
- P/ SER ACESSO, O DISPOSITIVO DEVE POSSUIR A TECNOLOGIA WI-FI INTEGRADA

WiMAX

- PADRÃO SEM FIO DE ALTA VELOCIDADE PARA REDES METROPOLITANAS (WMAN)
- CAPAZ D/ OFERECEER INTEROPERABILIDADE ENTRE OS EQUIPAMENTOS
- RAIO DE ATÉ 40 KM
- OPERA NO ESPECTRO DE FREQUÊNCIA 2.4 GHz, 3.5GHz e 10.3 GHz
- NECESSÁRIO CONCESSÃO DA ANATEL
- POSSUI 3 ESQUEMAS DE MODULAÇÃO: QAM-64, QAM-16 e QPSK



@mapasdathai



1.16 Questões Comentadas - Redes de Computadores - Parte 1 - MULTIBANCAS

#VamosPraticar#

Questões Comentadas – Diversas Bancas

48 - (IFSUL / IFSUL – 2009)

Sobre o Bluetooth, assinale a alternativa INCORRETA.

- Piconet é o nome dado a uma rede Bluetooth que consiste de um equipamento mestre e até sete escravos ativos.
- É um sistema de baixa potência com alcance de 10 metros e taxa de dados bruta de 1Mbps.
- Opera na frequência de 5 GHz, mesma banda do padrão IEEE 802.11a para redes wireless.

d) É padronizado pelo grupo de trabalho IEEE 802.15.

Comentários:

(a) Correto; (b) Correto; (c) Errado, ele opera na frequência de 2.4GHz – IEEE 802.11a opera na frequência de 5GHz; (d) Correto.

Gabarito: Letra C

#VamosPraticar#

Referências e links deste capítulo

1 Existe um quarto tipo bem raro em provas chamado

2 Aliás, a maioria das redes domésticas são Redes P2P. Eu tenho uma rede na minha casa para compartilhar arquivos entre o meu computador e o notebook da minha esposa. Logo, ambos os dispositivos fazem o papel de cliente e servidor simultaneamente.

3 Existem outras topologias, como a topologia em árvore, daisy chain, entre outros, mas não é o foco desse curso. Há também topologias híbridas, que combinam duas ou mais topologias.

4 Assim como a topologia em anel (que veremos adiante), está em desuso há muitos anos, mas continua sendo cobrada em concursos públicos.

5 Nó central é um dispositivo que concentra conexões – em geral, ele liga os cabos dos computadores de uma rede (Ex: Hub ou Switch).

6 Caso a banca não deixe explícito de qual tipo está tratando, considere que se trata de uma malha completa.

7 O BNC é usado para conectar a extremidade de um cabo a um dispositivo, mas existe também o conector T-BNC, usado para dividir uma conexão com em duas; e também o Terminador BNC, usado no final do cabo para impedir a reflexão do sinal.

8 Cada porta do switch possui um buffer (uma espécie de banco de memória) em que os dados são armazenados/enfileirados, não ocorrendo colisões, portanto não necessitando utilizar o Protocolo CSMA/CD.

9 Banda é a quantidade de bits que podem trafegar por uma conexão em uma determinada unidade de tempo, isto é, velocidade (Ex: 100Mbps).

- 10** Utilizar a topologia em estrela com um hub não adiantaria nada porque esse dispositivo tem topologia lógica em barramento.
- 11** Em geral, Bluetooth tem um caráter mais ad-hoc e Wi-Fi tem um caráter mais de infraestrutura (apesar de não ser obrigatório).
- 12** Se você usa teclado sem fio, provavelmente embaixo dele está informando a frequência 2.4 Ghz. Verifiquem aí :)
- 13** Atenção: alguns alunos enviaram reclamações pedindo para retirar o termo mestre/escravo da aula por ter cunho racista. No entanto, esse é o termo técnico utilizado em bibliografias consagradas e em questões de concurso, logo infelizmente não há como retirá-lo.
- 14** Na Dark Web, as páginas não usam os domínios tradicionais como .com, .org, .net, ou domínios nacionais como .br (para o Brasil). Em vez disso, muitos sites da Dark Web usam o domínio .onion (Exemplo
- 15** O nome
- 16** <http://www.instagram.com/professordiegocarvalho>